Why Not Privacy By Default?

WHY NOT PRIVACY BY DEFAULT?

Lauren E. Willis∗

We live in a Track-Me world, one from which opting out is often not possible. Firms collect reams of data about all of us, quietly tracking our mobile devices, our web surfing, and our email for marketing, pricing, product development, and other purposes. Most consumers both oppose tracking and want the benefits tracking can provide. In response, policymakers have proposed that consumers be given significant control over when, how, and by whom they are tracked through a system of defaults (i.e., "Track-Me" or "Do-Not-Track") from which consumers can opt out.

The use of a default scheme is premised on three assumptions. First, that for consumers with weak or conflicted preferences, any default chosen will be "sticky," meaning that more consumers will stay in the default position than would choose it if an affirmative action were required to reach the position. Second, that those consumers with a fairly strong preference for the opt-out position—and only those consumers—will opt out. Third, that where firms oppose the default position, they will be forced to explain it in the course of trying to convince consumers to opt out, resulting in well-informed decisions by consumers.

This article demonstrates that for tracking defaults, these assumptions may not consistently hold. Past experience with the use of defaults in policymaking teaches that Track-Me defaults are likely to be too sticky, Do-Not-Track defaults are likely to be too slippery, and neither are likely to be information-forcing.

These conclusions should inform the "Do-Not-Track" policy discussions actively taking place in the U.S., in the E.U., and at the World Wide Web Consortium. They also cast doubt on the privacy and behavioral economics literatures that advocate the use of "nudges" to improve consumer decisions about privacy.

I. INTRODUCTION

We live in a Track-Me[1] world, one from which opting out is, as a practical matter, often not possible. Firms collect reams of data about us for marketing, pricing, product development, and other uses. Sometimes we are knowing participants in the first stage of this process—a firm asks for information and we provide it, knowing roughly how that firm will use it. But much data collection is passive, invisible, and performed without explicit consent. We are rarely aware of the identities of passive data collectors or downstream users to whom our data may be transferred. And neither we nor the firms collecting data today know all the future uses to which our data may be put. Collection of data on the websites people visit, the content of their emails, and the movements of their mobile

∗ Robert S. Braucher Visiting Professor of Law, Harvard Law School and Professor of Law, Loyola Law School Los Angeles, lauren.willis@lls.edu. My thanks to Omri Ben-Shahar, Chris Hoofnagle, Paul Ohm, Jules Polonetsky, Paul Schwartz, Chris Soghoian, Lior Strahilevitz, participants at the 2013 Privacy Law Scholars Conference, and research assistant Natalie Kim.

1 This article uses "Track-Me" and "Do-Not-Track" to avoid the indeterminacy of "Opt-In" and "Opt-Out," and uses "tracking" in a colloquial sense to refer to all forms of personal data collection and use for commercial purposes, online and off. For a discussion of Do-Not-Track as a technical protocol, *see* DO NOT TRACK—UNIVERSAL WEB TRACKING OPT OUT, http://donottrack.us/ (last visited Aug. 1, 2013). Collection and use of personal data for law enforcement purposes is beyond the scope of this article.

phones have garnered the most media attention,[2] but as tracking technologies (e.g., facial recognition programs, eye tracking systems and geolocation sensors) become cheaper and more accurate, the amount of data collected passively and the uses to which it will be put will only increase.[3]

Although preferences for information privacy vary, wide majorities of people both express opposition to the extent of this data collection and have taken some steps to avoid being tracked.[4] They wish to avoid uses of their data that they experience as harmful (e.g., identity theft, price discrimination, negative employment consequences) as well as the more amorphous costs of a lack of privacy, the "creepy" feeling of being watched that creates a decreased space for individual experimentation and reflection key to personal growth.[5] Yet people also want the benefits that tracking can provide, such as online socializing and access to online content.[6]

In response, policymakers have proposed that consumers be given significant control over when, how, and by whom they are tracked through a system of defaults (i.e., "Track-Me" or "Do-Not-Track") from which consumers can opt out.[7] Ostensibly, this "notice and choice" regime is

2 Most websites track users, collecting information such as access time, visit duration, mouse movements and clicks. *See* Andrew Couts, *Top 100 Websites: How They Track Your Every Move Online*, DIGITAL TRENDS (Aug. 30, 2012), http://www.digitaltrends.com/web/top-100-websites-how-are-they-tracking-you/ (finding that the top 100 websites all track users in some way). Some providers of "free" email scan users' email text. *See, e.g.,* John Pallatto, *Google Defends Scanning E-Mail for Ad Links*, EWEEK (Apr. 23, 2004), http://www.eweek.com/c/a/Messaging-and-Collaboration/Google-Defends-Scanning-EMail-for-Ad-Links/ (explaining that Google scans email text of Gmail users for targeted ad purposes). Mobile data is often tracked through applications or by cell carriers themselves, then sold to third parties. *See, e.g.*, Olga Kharif & Scott Moritz, *Cell Carriers Sell Users' Tracking Data in $5.5 B Market*, DELAWAREONLINE (June 13, 2013), http://www.delawareonline.com/article/20130613/BUSINESS08/306130050/Cell-carriers-sell-users-tracking-data-5-5-B-market.

3 *See generally What They Know*, WALL ST. J., http://online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Aug. 1, 2013).

4 *See, e.g.*, Lee Rainie et al., *Anonymity, Privacy, and Security Online*, PewResearchCenter Report at 8, pewinternet.org/Reports/2013/Anonymity-online.aspx (Sept. 5, 2013) (86% of internet users have "taken at least one step to try to mask their behavior or avoid being tracked"); Chris Crum, *Googler: Nobody Wants to Be Tracked Online*, WEBPRONEWS (Apr. 2, 2012), http://www.webpronews.com/googler-nobody-wants-to-be-tracked-online-2012-04 (finding that nearly 85% of users think a business should not be able to track consumer activity on the business's website, even anonymously).

5 *See, e.g.*, Martha C. White, *Orbitz Shows Higher Prices to Mac Users*, TIME, June 26, 2012, http://business.time.com/2012/06/26/orbitz-shows-higher-prices-to-mac-users/#ixzz2iC0bd6Dehttp://business.time.com/2012/06/26/orbitz-shows-higher-prices-to-mac-users/ (describing negative consumer reaction to perceived price discrimination based on personal information); ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011) (arguing that privacy is often necessary for personal dignity, trust, and reputation, all of which preserve individual freedom to make one's own social, economic and political choices).

6 *See, e.g.*, Omer Tene & Jules Polonetsky, *Privacy In The Age Of Big Data: A Time For Big Decisions*, 64 STAN. L. REV. ONLINE 63 (2012), *available at* http://www.stanfordlawreview.org/online/privacy-paradox/big-data (listing significant benefits currently produced by tracking).

7 *See, e.g.*, The Do-Not-Track Online Act of 2013, S. 418, 113th Cong. (2013) (proposed legislation which would require the FTC to create an enforceable "mechanism by which an individual can simply and easily indicate whether the individual prefers to have personal information collected by providers of online services, including by providers of

motivated by a desire to satisfy diverse privacy preferences. Such an approach has deep normative roots; privacy itself has been conceptualized as a right of individuals "to determine for themselves when, how, and to what extent information about them is communicated to others."[8] Conveniently for policymakers, the use of tracking defaults in privacy policy also dodges the judgment calls required to resolve the conflict between people's desire for information privacy and their desire for tracking's benefits.[9]

Contested in policy circles today is whether to set Track-Me or Do-Not-Track as the default.[10] Three key assumptions taken from the behavioral economics literature underlie the debate.[11] First, that any default chosen will be "sticky," meaning that more consumers stay with the default than would explicitly choose to do so if forced to make a choice.[12] Second, that those consumers with a

mobile applications and services"); THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD, 11–22 (Feb. 2012) (proposing a Consumer Privacy Bill of Rights, which includes "Consumers have a right to exercise control over what personal data companies collect from them and how they use it.").

8 ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). This focus on individual choice may be misplaced, regardless of whether meaningful choice is possible. Social welfare and individual preferences about privacy may not be well-aligned, and if so, policymakers ought to make policy based on the social costs and benefits of tracking rather than based on a quest to satisfy preferences. But that debate is beyond the scope of this article.

9 *Cf.* JAMES P. NEHF, OPEN BOOK: THE FAILED PROMISE OF INFORMATION PRIVACY IN AMERICA 103-04 (2012) (explaining difficulty policymakers have with resolving the incommensurability of the costs and benefits of privacy).

10 A third possibility is forced choice, meaning consumers could not continue with the online or off-line activity from which data will be collected without affirmatively making choices about tracking. Under a forced choice regime, a consumer could not enter a store that tracks cellphones, view a website that tracks browsing activity, use a credit card at a retailer that tracks customer purchases or open a mobile device application that collects personal data, without first deciding whether to be tracked. Forced choice is largely ignored in policy discussions, perhaps because such frequent decisions would be burdensome, or because most consumers would respond with a reflexive "yes" click so as to move along in their daily activities rather than engage in reflective decisionmaking.

11 A fourth key assumption is that defaults imposed by law can and will be enforced. These assumptions may be naive, as the EU, Israeli, and, in the U.S., the Children's Online Privacy Protection Act (COPPA) experiences suggest. *See, e.g.*, Maurizio Borghi et al., *Online Data Processing Consent Under EU Law: A Theoretical Framework and Empirical Evidence from the UK,* 21 INT'L. J. L. & INFO. TECH. 109 (Summer 2013) (finding widespread noncompliance with EU and UK law requiring user consent prior to data collection); Michael Birnhack & Niva Elkin-Koren, *Does Law Matter Online? Empirical Evidence on Privacy Law Compliance,* 17 MICH. TELECOMM. & TECH. L. REV. 337 (2011) (finding widespread noncompliance with Israeli law requiring notice to users about data collection); EUROPEAN NETWORK AND INFO. SEC. AGENCY, PRIVACY CONSIDERATIONS OF ONLINE BEHAVIOURAL TRACKING, 16 (Oct. 2012), http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking (finding that EU law requiring user consent prior to tracking is not being enforced by the EU or member countries); Danah Boyd*, Why Parents Help their Children Lie to Facebook About Age: Unintended Consequences of the 'Children's Online Privacy Protection Act',* 16 FIRST MONDAY 11 (2011), http://firstmonday.org/ojs/index.php/fm/article/view/3850 (finding widespread circumvention of COPPA's default that websites cannot collect information about children unless their parents opt out). To present the strongest case for tracking defaults, this Article assumes they would be enforceable and enforced, but nonetheless finds that tracking defaults are unlikely to achieve policymakers' professed aims.

12 *See, e.g.*, Cass R. Sunstein, *Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules: A Triptych* 9 (Harvard Law Sch. Working Paper Series, May 19, 2013) (working paper), *available at*

preference for the opt-out position —and only those consumers—will opt out.[13] Third, that where firms oppose the default position, they will be forced to explain it in the course of trying to convince consumers to opt out, resulting in well-informed decisions by consumers.[14] In behavioral economics parlance, tracking defaults are expected to be sticky "policy defaults" (selected with an aim to nudge people with weak or unformed preferences toward the default position)[15] or information-forcing "penalty defaults" (selected with an aim to educate people about the default and opt-out positions).[16]

This Article demonstrates one reason why the debate over tracking defaults is misguided – the assumptions underlying the use of defaults in policymaking are unlikely to hold in the personal data tracking context. Defaults can be too sticky (meaning that consumers who, were they well-informed, would prefer to opt out, instead stick with the default) or too slippery (meaning that consumers who, were they well-informed, would prefer the default position, instead opt out), and are not always information-forcing. Defaults favored by firms are often surrounded by a powerful campaign to keep consumers there, but defaults set contrary to firm interests can be met with an equally powerful campaign to drive consumers to opt out. Firms can bolster the mechanisms behind the inertia that leads consumers to stick with defaults, or can weaken them to induce consumers to opt out. Rather than forcing firms to facilitate consumer exercise of informed choice, many defaults leave firms with opportunities to play on consumer biases or confuse consumers into sticking with or opting out of the default.

Thus, whether a tracking default is sticky or slippery, informative or uninformative will depend on whether firms' interests are aligned with the default. Firms can increase or decrease transaction barriers to opting out and frame the issue to influence consumer decisions. To counter firm manipulation, the law can impose "altering rules"[17]—rules governing the process by which consumers can opt out--and "framing rules"[18]—rules governing the presentation of the default to consumers. But normative, legal, and practical constraints limit altering and framing rules, and the

---

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171343 ("In the domain of privacy on the Internet, a great deal depends on the default rule.").

13 *See, e.g.*, Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives From Law, Computer Science And Behavioral Economics*, 82 NOTRE DAME L. REV. 583, 633 (2006) (suggesting penalty defaults for privacy settings to protect uninformed users yet allow "well-informed individuals" to opt out).

14 *See, e.g.,* Lilian Edwards & Ian Brown, *Data Control and Social Networking: Irreconcilable Ideas?*, *in* HARBORING DATA: INFORMATION SECURITY, LAW AND THE CORPORATION 22 (A. Matwyshyn ed., 2009) ("A general rule that privacy settings be set at the most privacy-friendly setting when a profile is first set up . . . would inform all users that privacy settings do exist, and force them to learn how to make use of them before they moved on to networking . . . .").

15 *See, e.g.*, Craig R. M. McKenzie et al., *Recommendations Implicit in Policy Defaults*, 17 PSYCH. SCI. 414, 414 (2006).

16 *See* Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 91 (1989); *see also* Janger & Schwartz, *supra* note__, at 1239 (dubbing penalty defaults "information-forcing defaults").

17 *See* Ian Ayres, *Regulating Opting Out: An Economic Theory of Altering Rules*, 121 YALE L. J. 2032 (2012).

18 *See* Elizabeth F. Emens, *Changing Name Changing: Framing Rules and the Future of Marital Names*, 74 U. CHI. L. REV. 763, 840 (2007).

strongest such rules within these constraints can be outmaneuvered by firms with the means and motivation to do so.

Unless robust competition over protecting consumer privacy develops in the marketplace—an unlikely prospect—firms will generally prefer for consumers to be in the Track-Me position. Because firms can influence people's responses to tracking defaults, most Track-Me defaults are likely to be too sticky and many Do-Not-Track defaults are likely to be too slippery. Further, neither the consumers who stick with Track-Me defaults nor those who opt out of Do-Not-Track defaults will necessarily be making well-informed decisions. Therefore, personal data tracking defaults are unlikely to facilitate the satisfaction of heterogeneous consumer preferences or produce informed resolution of the conflict between people's desire for information privacy and their desire for the benefits produced by their data.

Other privacy scholars have been skeptical of the idea that a notice-and-choice regime could produce robust individual decision-making about personal data privacy.[19] Yet their critiques have not confronted and have even equivocated in the face of the assumptions about defaults made by the standard behavioral economics literature.[20] Some of them continue to advocate defaults, but on norms-setting grounds rather than as sticky policy defaults or information-forcing penalty defaults[21] But for defaults to set these norms, the signal must be clear. Experiences with other default rules give reason to think that tracking default settings opposed by firms will be accompanied by a great deal of noise, noise calculated to confuse the signal and make the opposed default slippery. Only tracking defaults that firms embrace will be sticky.

This Article fills the current intellectual gap with an understanding of the limits of defaults and surrounding altering and framing rules and, given these limits, how the dynamic responses of firms to defaults can undermine policymakers' aims. More broadly, it casts doubt on the use of "nudges"[22]

19 The classic article on personal information tracking defaults is Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219 (2001). *See also, e.g.,* Paul M. Schwartz, *Privacy and Democracy in Cyberspace,* 52 VANDERBILT L. REV. 1609, 1660-63 & 1681-85 (1999) (critiquing the individual choice model of privacy); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARVARD L. REV. 1880 (2013) (same).

20 *See, e.g.,* Schwartz, *supra* note __ at 1686-87 (suggesting that a default of minimal data disclosure would allow individuals to "personalize their privacy levels"); Paul M. Schwartz , *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2100 (2004) ("This Article prefers an opt-in default because . . . it would place pressure on the better-informed party to disclose material information about how personal data will be used. This default promises to force the disclosure of hidden information about data-processing practices."); Solove, *supra* note __ at 1900 ("[P]rivacy self-management should not be abandoned").

21 *See, e.g.,* Solove, *supra* note __ at 1903 ("The law should develop and codify basic privacy norms… in a form like the Uniform Commercial Code (UCC), where certain default rules can be waived."); Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising,* 281 MINN. J. L. SCI. & TECH 281, 341 (2012) (suggesting that tracking defaults be used to signal and effectively set social norms about what information should and should not be shared, with whom, and under what conditions).

22 *See* Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* 6 (Yale 2008). (defining a "nudge" as a policy tool that "alters people's behavior in a predicable way without forbidding any options or significantly changing their economic incentives.").

in policymaking to help people make better choices about information privacy.[23] Track-Me and Do-Not-Track defaults might pave the political path to a better system for regulating personal data tracking, but also might defuse the political will to implement better regulation.

This article proceeds as follows: Part II describes the theoretical and empirical foundation for the use of defaults in policymaking: the mechanisms that can make defaults sticky, the conditions under which these mechanisms are likely to operate, and the use of altering and framing rules to calibrate the stickiness of defaults. Part III explains how policymakers appear likely to translate the theories behind the use of defaults as policy tools to the personal data tracking arena, including the contours of the defaults and altering and framing rules policymakers are likely to select. Part IV looks to defaults in other fields to assess when defaults do and do not work in practice. Based on these experiences, Part V considers how tracking defaults are likely to play out, predicting that Track-Me defaults are likely to be overly sticky and Do-Not-Track defaults are likely to be overly slippery. Part V also explains why altering rules, framing rules, and competition have limited potential to change these dynamics. Part VI concludes with an exploration of the potential political consequences of using defaults in information privacy policy.

II. DEFAULTS IN THEORY

A default is a setting or position that has been preselected, but can be altered. Many websites, mobile phones, mobile applications and other devices and programs that can facilitate or inhibit tracking are pre-set to allow tracking today, such that "Track-Me" is a quasi-default.[24] These settings are not full-fledged defaults, in that opting out is not always possible—some devices and programs cannot be used without tracking enabled and some trackers track consumers even when program or device settings are in the Do-Not-Track position.[25] But consumers can opt out of some tracking to

23 A burgeoning literature advocates the use of nudges to encourage people to make better privacy decisions. *See, e.g.*, Rebecca Balebako et al., *Nudging Users Towards Privacy on Mobile Devices*, *in* Proceedings of the 2nd International Workshop on Persuasion, Influence, Nudge & Coercion Through Mobile Devices (2011); M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027 (2012); Yang Wang et al., *"It made me think twice": A Field Trial of a Facebook Privacy Nudge*, Paper in the Privacy Law Scholars Conference (2013); Alessandro Acquisti, *Nudging Privacy: The Behavioral Economics of Personal Information*, 7 IEEE 82 (2009).

24 *See, e.g.,* Claire Cain Miller, *How to Opt Out of Google's Plan to Use Your Name and Comments in Ads,* N.Y. TIMES (Oct. 14, 2013) (discussing how some of Google's settings are set by default to Track-Me); Andrew Couts, *Are Apple's iOS 7 privacy settings purposefully misleading, or just a mess?, Digital Trends* (Sept. 29, 2013) (discussing iPhone defaults set to enable tracking),

http://www.digitaltrends.com/mobile/apple-your-ios-7-privacy-settings-are-a-mess/#ixzz2iCafwri3. Although most tracking settings are set by default to Track-Me, a few are not. *See, e.g.*, *Safari Blocks all Cookies by Default*, APPLE SUPPORT COMMUNITIES, https://discussions.apple.com/thread/4040376?start=0&tstart=0 (last visited Aug. 1, 2013).

25 *See, e.g.,* Peter Maass & Megha Rajagopalan, *That's No Phone. That's My Tracker,* PROPUBLICA, July 13, 2012 (reporting that cellphone tracking canot be turned off, even if phone is powered down); Google: Gmail users 'have no legitimate expectation of privacy', Rt.com (Aug. 13, 2013), http://on.rt.com/47y0ku (Gmail cannot be used without allowing Google to scan email content for various purposes); Balebako et al., *supra* note **Error! Bookmark not defined.** (finding that trackers continue to track users who have turned on Do-Not-Track browser settings); Katy Bachman, *Yahoo Says No to Microsoft's 'Do Not Track' Browser, Others expected to follow suit*, ADWEEK (Oct. 26, 2012) (reporting that Yahoo and others

some extent. Consumers can delete some types of cookies from their browsers or install software that blocks some internet and cellphone tracking.[26] They can change tracking options on their Facebook, Twitter, or Google accounts.[27] They can set their browsers or install cellphone apps to tell advertising networks not to serve them behaviorally targeted ads.[28]

The first premise behind the use of defaults in policymaking is that defaults are sticky, and today's "Track-Me" quasi-default supports that premise. While a majority of consumers claim that they have taken at least some steps to opt out of internet tracking,29 these claims are almost certainly more aspirational than representational. 30 It seems extremely unlikely that many consumers successfully opt out in a thoroughgoing way on each device, browser, and app through which they are tracked. Currently, about 17% of U.S. Firefox users have "Do-Not-Track" activated.[31] But fewer than 10% of consumers even know that common mobile phone apps track them.[32] Although claims by firms that they have data on nearly all Americans and can track nearly all internet users may likewise be exaggerated, these claims are unlikely to be very far off the mark. [33] Most consumers stick with most Track-Me positions.

---

will not honor a Do-Not-Track signal received from an internet explorer browser).. Firefox is developing technology to prevent the placement of cookies on computers when the browser is set to Do-Not–Track, but browsers are unlikely to win a technology war with trackers, which in the past have evaded technological attempts to maintain privacy. *See* Chris Jay Hoofnagle, *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. J.L. & PUB. POL'Y 273 (2012)..

26 See, e.g., Alan Henry, *Everyone's Trying to Track What You Do on the Web: Here's How to Stop Them*, LIFEHACKER (Feb. 22, 2012), http://lifehacker.com/5887140/everyones-trying-to-track-what-you-do-on-the-web-heres-how-to-stop-them; Erica Naone, *Smartphone Apps: How to Spot and Stop Firms Tracking Your Phone*, CHRISTIAN SCIENCE MONITOR, May 5, 2011, at __.

27 *See, e.g.,* Alan Henry, *Facebook Is Tracking Your Every Move on the Web; Here's How to Stop It*, LIFEHACKER (Sept. 26, 2011), http://lifehacker.com/5843969/facebook-is-tracking-your-every-move-on-the-web-heres-how-to-stop-it; Ryan Tate, *How Google Spies on Your Gmail Account (And How To Stop It)*, GAWKER (May 11, 2011), http://gawker.com/5800868/how-google-spies-on-your-gmail-account-and-how-to-stop-it; Alan Henry, *Twitter Wants to Start Tracking you on the Web, Here's How to Opt-Out*, LIFEHACKER (July 3, 2013), http://lifehacker.com/twitter-wants-to-start-tracking-you-on-the-web-heres-661569459.

28 *See* ADCHOICES, http://www.youradchoices.com; Wendy Davis, *New App Lets Mobile Users Opt Out Of Behavioral Targeting*, ONLINE MEDIA DAILY (Apr. 11, 2011), http://www.mediapost.com/publications/article/197792/new-app-lets-mobile-users-opt-out-of-behavioral-ta.html#axzz2Z4TIj0jL.

29 *See* Rainie et al., *supra* note __ at 8 (86% of consumers claim to have taken at least one step to avoid being tracked).

30 Consumers claim to engage in significantly more privacy-protective online behavior than they truly do. Carlos Jensen et al., *Privacy practices of Internet users: Self-reports versus observed behavior*, 63 INT. J. HUMAN-COMPUTER STUD. 203 (2005).

31 Alex Fowler, *Mozilla's New Do Not Track Dashboard: Firefox Users Continue to Seek Out and Enable DNT*, MOZILLA PRIVACY BLOG (May 3, 2013), https://blog.mozilla.org/privacy/2013/05/03/mozillas-new-do-not-track-dashboard-firefox-users-continue-to-seek-out-and-enable-dnt/.

32 David Talbot, *Using Crowdsourcing to Protect Your Privacy*, MIT TECH. REV. (Apr. 2, 2012), http://www.technologyreview.com/news/427390/using-crowdsourcing-to-protect-your-privacy/page/2/.

33 While consumers claim to engage in privacy-protective behavior, firms that collect personal data claim to have extensive data on most U.S. adults. *See* Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES, June 16, 2012. One firm claims that it can use digital fingerprinting technology, a technology that does not depend on cookies

Why is today's Track-Me quasi-default so sticky? Using today's Track-Me position as an example, this Part explains the mechanisms that can make defaults sticky and the conditions that facilitate the operation of these mechanisms. It then elaborates on how academics have theorized that defaults, and altering and framing rules to fine-tune those defaults, might be used in policymaking so as to nudge people toward particular positions and/or educate people about particular choices.

A. MECHANISMS THAT MAKE DEFAULTS STICKY

Three types of mechanisms can operate to make defaults sticky: (1) transaction barriers, (2) judgment and decision biases, and (3) the preference-forming effects of defaults.[34] Not every mechanism will affect every default, but where a default is sticky, one or more of these mechanisms are at work.

1. Transaction Barriers

The first type of mechanism that can make a default sticky is transaction barriers. Transaction barriers here include (a) costs, (b) confusion, and (c) the belief that opting out is futile. Opting out of tracking today is impeded by each of these barriers.

a. Where the real or perceived *costs* of opting out appear not worth the benefits, it is rational to stick with the default. To opt out of tracking today, consumers must find the opt-out procedure, if one exists, and execute the steps for opting out, such as installing a program, changing settings, or completing an online form. Even when not onerous, this process must be completed for each device (e.g., cellphone, tablet, desktop) and program through which one can be tracked.35 In some instances, consumers must separately opt out of tracking by each tracker. For example, some advertising networks permit consumers to opt out of receiving behavioral advertising, but the procedure requires consumers to individually select each advertising network from which they would like to opt out.[36] Further, some of these steps must be repeatedas firm privacy policies change, as trackers develop new ways to evade consumer attempts to opt out, and as consumers upgrade devices or software.37 In addition, if a consumer deletes all cookies, cookies that had been sending

---

and can identify mobile devices in addition to computers, to identify 98% of internet users. *See* Adam Tanner, *The Web Cookie Is Dying. Here's The Creepier Technology That Comes Next*, FORBES, June 17, 2013.

34 For a more detailed explanation of some of the mechanisms that can make defaults sticky, see Lauren E. Willis, *When Nudges Fail: Slippery Defaults*, U. CHI. L. REV.. (forthcoming 2013).

35 *See, e.g.*, http://www.coxdigitalsolutions.com/privacy-policy/consumer-opt-out-program/ ("If you use more than one type of browser or more than one computer to access the Internet, you will have to opt out in each browser and on each computer that you use.").

36 *See, e.g., Opt Out from Online Behavioral Advertising*, ADCHOICES, http://www.aboutads.info/choices/#completed (last visited Aug. 1, 2013).

37 *See, e.g.,* http://www.coxdigitalsolutions.com/privacy-policy/consumer-opt-out-program/ ("You may need to opt out repeatedly. If you delete or otherwise alter your browser's cookie file (including upgrading certain browsers) you may need to opt out again.")

do-not-track messages must be reinstalled38; if a consumer changes browser settings to allow tracking so as to facilitate a particular transaction, she must go back and change settings again to return to a do-not-track position.

Should existing transaction costs not be a sufficient deterrent, firms can add other costs, such as conditioning cellphone app downloads or email use on permission to gather user data or scan user emails.[39] Short of conditioning access on tracking, firms can make refusing to be tracked costly. Many websites warn consumers: "If you turn cookies off, you will not have access to many features that make your user experience more efficient and some parts of our website will not function properly."[40] .

b. Three types of *confusion* can contribute to the stickiness of defaults. The first is confusion about the opt-out process, such that those who attempt to opt out fail to do so. The second is confusion about the value to which the default is set, and more particularly thinking that the default meets the consumer's preferences when it does not. The third is confusion about the status of a default position, thinking that the position is a mandate and thus a position from which one cannot opt out.

All of these types of confusion may contribute to the stickiness of today's Track-Me quasi-default. Many consumers think they know more about technology related to privacy than they do.[41] Popular misconceptions include thinking that turning cellphones "off" disables phone tracking and that changing browser settings or deleting cookies disables internet tracking.[42] The result is that consumers who attempt to opt out of tracking today often do not manage to do so to the extent they desire—and often mistakenly believe they have done.[43] For example, as facebook's privacy settings became more granular, they also became more confusing, with the result that fewer users opted out of the defaults.[44]

---

38 *Id.*

39 *See* Adrienne Porter Felt et al., *Android Permissions: User Attention, Comprehension, and Behavior, Symposium on Usable Privacy and Security* (SOUPS) 2012 (app downloads); Rt.com, *supra* note __ (Gmail).

40 *Consumer Online Privacy Frequently Asked Questions*, U.S. BANK, https://www.usbank.com/privacy/faq.html#4 (last visited July 30, 2013). See also Disney Registration Cookies Policy, https://registration.disneyinternational.com/cookiepolicy.htm?p=130&fullScreen=true (similar warning language); Information about Cookies on Monster, http://inside.monster.com/cookie-info/inside2.aspx (same).

41 Jensen et al., *supra* note **Error! Bookmark not defined.**.

42 *See* Alex Colon, *Is Your Phone Tracking You Even with Location Services Turned Off?*, PCMAG, Apr. 25, 2011 (turning off a phone does not stop tracking); Hoofnagle, *supra* note **Error! Bookmark not defined.** (changing browser settings or deleting cookies does not prevent tracking).

43 Pedro G. Leon et al., *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising* 1, 4 (Carnegie Mellon Univ., Working Paper , Oct. 31, 2011), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/ CMUCyLab11017.pdf ("[M]ultiple participants opted out of only one company . . . despite intending to opt out of all. Others mistook the [registration] page . . . as the opt out page."). *See also* Janger & Schwartz, *supra* note **Error! Bookmark not defined.**, at 1241 (noting that confusing and misleading privacy notices are designed to lead to consumer inaction).

44 Stutz et al. at 21-25,

Other consumers may not try to opt out, because although they would prefer not to be tracked, they believe that the default permits little tracking. Many people do not know that firms can track their internet use, scan their email text, and follow their device movements for commercial purposes.[45] [I]n one survey nearly all respondents were surprised that a popular flashlight app sent the user's unique cellphone ID and precise location to advertisers.[46] Most consumers falsely believe that the law significantly restricts collection of consumer information[47] and that the existence of a "Privacy Policy" means that their information is not shared with third parties.[48] Mistaken about what happens if they do nothing, even consumers who prefer not to be tracked have no reason to opt out.

Others know about tracking, but are unaware of the (albeit limited) ways in which they can opt out.[49] Invisibility of the option to opt out inevitably leads to sticking with the default.

c. Where opting out of a default appears to be *futile*, a consumer might choose not to even try. Some consumers today understand that opting out of the Track-Me position today is not entirely possible.[50] Others, perhaps accurately given the confusion just discussed, believe that they lack the expertise to manage to opt out entirely.51 For example, most users find Facebook privacy settings

45 *See, e.g.*, Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It* (Working Paper, Sept. 29, 2009), http://ssrn.com/abstract=1478214 (finding that only 33% of users in 2009 survey knew that their internet use could be tracked across multiple websites without their consent); Adario Strange, *Google's Snooping Gmail the Target of Microsoft's Latest 'Scroogle' Attack*, ITPROPORTAL (Feb. 8, 2013), http://www.itproportal.com/2013/02/08/googles-snooping-gmail-the-target-of-microsoft-latest-scroogle-campaign/ (reporting that fewer than 30% of Gmail users surveyed knew that their email text was scanned for behavioral advertising purposes); Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES, July 14, 2013 (reporting that shoppers were surprised that their movements within a store were monitored through their cellphones).

46 Talbot, *supra* note 32.

47 *See* Turow et al., *supra* note 32, at 21, Tbl. 9 (2009).

48 Ilana Westerman, *What Misconceptions Do Consumers Have about Privacy?*, PRIVACY PERSPECTIVES (June 3, 2013), https://www.privacyassociation.org/privacy_perspectives/post/what_misconceptions_do_consumers_have_about_privacy; Jensen et al., *supra* note **Error! Bookmark not defined.**, at 223.

49 Two-thirds of consumers are unaware of options they have to limit how much information is collected about them. *See* KRISTEN PURCELL ET AL., SEARCH ENGINE USE 2012 (PEW INTERNET & AMERICAN LIFE PROJECT 2012). *See also Internet Users' Response to Consumer Online Privacy*, ANNALECT (Mar. 14, 2012), http://annalect.com/wpcontent/uploads/2012/06/Consumer_Online_Privacy_Whitepaper.pdf (finding 22% of users aware of some ability to opt out of tracking today).

50 Rainie, *supra* note __ at 12.

51 See, e.g., Blasé Ur et al., *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising* 8-9 (Carnegie Mellon Univ., Working Paper, July 13, 2012), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12007.pdf (reporting that in response to questions about opting out of behavioral advertising, many consumers expressed uncertainty about how to opt out); Yet Another OPT OUT You Should Think About, Oct. 20, 2013, available at http://www.boxlour.com/?p=319 ("Typically the process to opt out of something is not as easy as a "click here" button. In fact, they are literally banking on most of us getting so confused on the whole "opt out" process that we eventually give up. And give up we do.").

difficult to use.52 Rather than engage in futile attempts to opt out of the default, these consumers might not even try.53

2. Judgment and Decision Biases

The second type of mechanisms that can make defaults sticky is judgment and decision biases. Some biases are frequently associated with defaults, including (a) salience effects, (b) omission bias, (c) loss aversion and the endowment effect, and (d) procrastination and decision avoidance. But a closer look at the operation of tracking defaults reveals that nearly *any* type of bias might be invoked to favor a default, provided the conditions exist that facilitate the operation of biases, discussed further below. In the case of tracking, for example, (e) excessive discounting, (f) choice bracketing, (g) the illusion of control, and (h) the sunk costs fallacy all may contribute to the stickiness of today's Track-Me quasi-default.

a. Salience effects, meaning the tendency for salient information to disproportionately affect judgments and non-salient information to be ignored,[54] can result in sticking with a default even when the default and opt-out are not entirely invisible, but are simply not brought to mind.

The salience of tracking strongly influences people's privacy-related actions. One experiment found that consumers who are reminded of the privacy implications of disclosure disclose little, but those who are not reminded appear to forget about privacy—many will reveal socially stigmatized and even illegal behavior.[55] In the real world, tracking is rarely salient, in part because tracking occurs while a consumer is focused on something else–using a mobile phone, the internet, or the like. In addition, tracking may not be salient due to "warning fatigue". For example, some smartphone users who do know that apps collect personal information have become so habituated to fine print disclosures that they have stopped reading the app permissions lists.[56]

b. Omission bias, favoring inaction over action, is related to salience effects in that actions are more salient than omissions. People are more likely to blame themselves about a poor outcome when they make an active decision to opt out of a default than when the outcome is caused by

52 *See* Mary Madden, *Privacy Management on Social Media Sites*, PEW 2–3 (2012), http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx.

53 *See, e.g.,* Blasé Ur et al., *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising* 7 (Carnegie Mellon Univ., Working Paper, July 13, 2012), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12007.pdf (quoting consumer: "It makes me want to go home and delete all my cookies, but then I know that's not gonna help much."); Maria Karyda & Spyros Kokolakis, *Privacy Perceptions among Members of Online Communities in* DIGITAL PRIVACY 253, 263 (Acquisti et al, eds. 2010) (discussing consumer sentiments that user attempts to obtain privacy on the internet are futile).

54 *See, e.g.*, T. Hossain & J. Morgan, *Plus Shipping and Handling: Revenue (Non) Equivalence in Field Experiments on eBay*, 62 ADVANCES IN ECON. ANALYSIS & POL'Y 1, 20 (2006).

55 Leslie John et al., *Strangers on a Plane*, 37 J. CONSUMER RES. 858 (2011).

56 *See* Felt et al., *supra* note 39.

having remained in the default.[57] If both action and inaction involve some risk of negative consequences, people may stick with the default to avoid future regret.

Opting out of tracking today often involves clear negative consequences such as loss of website functionality or access to social media. Sticking with tracking involves a risk of unknowable probability of potential future harms such as identity theft, price discrimination, and restricted sace for personal development. Thus, unless a consumer believes that the costs of being tracked greatly exceed the benefits, she might not act to opt out, because opting out could lead to some losses *and* self-blame for those consequences, whereas staying put could lead to other losses but avoids self-blame.[58]

c. Loss aversion means weighing losses more heavily than gains against some reference point.[59] *The endowment effect*, placing a higher value on what one already possesses (or perceives oneself as possessing) than on the same thing when one does not possess it, is a manifestation of this.[60] When the default forms the reference point, these biases favor the default.

Research demonstrates an almost absurdly strong endowment effect for privacy. On average, people are willing to pay much more to keep data they are told is private that way, compared to what they will pay to obtain privacy when told that the default is for that data to be public; subjects in one experiment "were five times more likely to reject cash offers for their data if they believed that their privacy would be, by default, protected, than if they didn't enjoy such belief."[61] Thus, to the extent that consumers know they are currently in a Track-Me position, these biases favor that position.

d. Procrastination and *decision avoidance* are biases triggered when decisions or actions appear difficult. These biases can cause people to procrastinate indefinitely or to affirmatively decide not to make any decision, either of which could lead to sticking with the default.[62]

Procrastination and decision avoidance likely contribute to the stickiness of tracking defaults today for several reasons. First, the opt-out decision is difficult. Each time they make a decision about whether to opt out of a particular form of tracking, consumers must trade off incommensurate costs and benefits (e.g., the more tangible costs of forgoing access to internet

57 *See, e.g.*, Jonathan Baron & Ilana Ritov, *Reference Points and Omission Bias*, 59 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 475, 478 (1994).

58 *Cf.* David A. Asch et al., *Omission Bias and Pertussis Vaccination*, 14 MED. DECISION MAKING 118, 120–21 (1994).

59 *See, e.g.*, William Samuelson & Richard Zeckhauser, *Status Quo Bias in Decision Making*, 1 J. RISK & UNCERTAINTY 7, 19, 31 (1988).

60 Russell Korobkin, *Wrestling with the Endowment Effect, or How to Do Law and Economics Without the Coase Theorem* (UCLA Sch. of Law, Law-Econ Research Paper, Paper No. 13-10, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2289574.

61 *See* Alessandro Acquisti et al., *What Is Privacy Worth* 3, *in* 21ST WORKSHOP ON INFORMATION SYSTEMS AND ECONOMICS (2009), *available at* http://www.futureofprivacy.org/wp-content/uploads/2010/07/privacy-worth-acquisti-FPF.pdf .").

62 *See, e.g.*, Ted O'Donoghue & Matthew Rabin, *Choice and Procrastination*, 116 Q.J. ECON. 121, *passim* (2001);Christopher J. Anderson, *The Psychology of Doing Nothing: Forms of Decision Avoidance Result From Reason and Emotion,* 129 PSYCHOL. BULL. 139, *passim* (2003).

content or customization against the intangible benefits of increased space for personal experimentation and growth).[63] Second, opting out is costly;, as noted above, it requires consumers to navigate an opt-out process for each device or program that may be tracking them, steps that must be periodically revisited. Third, as explained above, opting out today is not entirely possible; some tracking is practically unavoidable, and some consumers know it. Rather than making a difficult decision over and over again, or starting an endless and futile battle against trackers, some consumers might procrastinate taking action or even affirmatively decide not to make any decision, the effect of which is to stay in the default position.64

e. Excessive discounting refers to people's tendency to prefer a much smaller gain now to a larger gain later and to prefer a sure gain to an uncertain but probabilistically much larger gain.[65] When opting out of a default entails definite upfront costs and uncertain future benefits, discounting over time and certainty will incline people to remain with the default.

The time and effort required to opt out of tracking today is immediate and certain. The benefits are in the future and uncertain, particularly given that future uses of information are unknown.[66] Thus, discounting may bolster today's Track-Me position.

f. Choice bracketing refers to whether a decision is evaluated in isolation or as part of a larger set of decisions.[67] Health-related decisions present an intuitive example. If the choice to eat a dessert or go for a run is made in isolation, the benefits of the dessert and costs of the run might easily outweigh the trivial incremental effect of each on health. Yet, the cumulative effect of these daily decisions can be enormous. Someone who views each choice in isolation might make less healthy choices than someone who mentally brackets decisions about diet, exercise, or health broadly.[68] Similarly, tracking decisions can be conceived narrowly or broadly. One consumer might make each decision in isolation, considering whether to permit a particular entity to track her at a particular moment in time. Another consumer might conceptualize each tracking decision as part of a broader choice about whether to allow herself to be tracked by any entity anytime. Firms are able to connect data gathered from a variety of sources–off-line, on-line, and from mobile devices–about a single

63 *See, e.g.*, Acquisti et al., *What Is Privacy Worth*, *supra* note 61, at 5–6 (discussing incommensurate tradeoffs consumers must make in the course of privacy-related decisions).

64 *Cf.* Chad Proell & Stephen Sauer, *"Stock" Options: The Debilitating Effects of Autonomy and Choice on Self-perceptions of Power* , 23 J. OF BUSINESS & BEHAV. SCIENCES (2011) (feelings of powerless lead to inaction).

65 *See, e.g.*, Yaacov Trope & Nira Liberman, *Construal-Level Theory of Psychological Distance*, 117 PSYCHOL. REV. 440, *passim* (2010) (explaining the tendency for people to discount over psychological distance, including over time and over uncertainty).

66 *See, e.g.*, Alessandro Acquisti & Jens Grossklags, *Uncertainty, Ambiguity and Privacy*, COMMUNICATIONS & STRATEGY, Special Issue on Privacy, 6 (2012) ("[A]n individual who is facing privacy sensitive scenarios may be uncertain about the values of possible outcomes and their probability of occurrence, and . . . sometimes she may not even be able to form any beliefs about those values and those probabilities."); NEFH, supra note __ at 126-29 (explaining that consumers cannot know how their information will be used or how those uses will affect them in the future).

67 Daniel Read et al., *Choice Bracketing*, 19 J. OF RISK & UNCERTAINTY 171 (2000).

68 *Cf. id.* at 171 (using example of decisions about smoking cigarettes).

consumer, collected over time.[69] Thus, the benefits of privacy and costs of a lack of privacy depend on the whole of privacy, not its parts, leaving uncertain whether tracking by any particular party or of any particular type of information will tip the scales.[70] Because the marginal negative impact of tracking by any one tracker is negligible, bracketing the choice narrowly could lead to a decision to allow tracking. Broad choice bracketing is more likely to result in selecting a Do-Not-Track position because the entirety of potential harms from tracking looms larger.

People often accept the bracketing implicit in a decision's presentation,[71] and many tracking decisions today are presented in a narrow form—e.g., Would you like to opt out of "tailor[ed] ads" from Twitter?[72] Rather than presenting the user with a single broad opt-out choice, a single device or program typically requires opting out of a series of particular types of tracking.[73] Even where broader choices are presented, such as in browser settings, trackers can ask consumers to alter that setting as to a particular website, a narrow choice. Thus, narrow choice bracketing may fortify today's Track-Me position.

g. The illusion of control is a bias that can lead people to take on more risk than they otherwise would,[74] and therefore might encourage consumers to stick with a risky default, if surrounding circumstances invoke the illusion. An example of the illusion is the common belief that one is less likely to experience an accident when one is driving than when one is a passenger, regardless of driving skill.[75]

Perceptions of control strongly affect privacy decision-making. Consumers who feel more in control of the exchange of their information with firms are more willing to allow those firms to collect more of their personal information.[76]Giving consumers the illusion of more control leads

69 *See, e.g.,* Somini Sengupta, *What You Didn't Post, Facebook May Still Know*, NY TIMES, March 25, 2013 (describing aggregation of on-line and off-line data about individual consumers); Claire Cain Miller & Somini Sengupta, *supra* note __ (describing aggregation of on-line and mobile data about individual consumers).

70 *Cf.* Solove, *supra* note __ at 1889-90 (dubbing this the "aggregation effect").

71 *Id.* at 188 (When "choices come to [people] one at a time, they will bracket them narrowly, and if choices come to them collectively, they will bracket more broadly.").

72 *See* Henry, *supra* note 27.

73 *See, e.g.,* Jason D. O'Grady, *Four privacy settings you should enable in iOS 7 immediately*, ZDNET (Sept. 19, 2013), http://www.zdnet.com/four-privacy-settings-you-should-enable-in-ios-7-immediately-7000020902/.

74 *See, e.g.*, M. S. Horswill & Frank P. McKenna, *The Effect of Perceived Control on Risk Taking*, 29 J. OF APPLIED SOCIAL PSYCHOL. 377 (1999); Ellen J. Langer, *The Illusion of Control*, 32 J. OF PERSONALITY & SOCIAL PSYCHOL. 311 (1975).

75 Frank P. McKenna, *It Won't Happen to Me: Unrealistic Optimism or Illusion of Control?*, 84 BRITISH J. OF PSYCHOL. 39, 39–50 (1993).

76 Nadia Olivero & Peter Lunt, *Privacy Versus Willingness To Disclose In E-Commerce Exchanges: The Effect Of Risk Awareness On The Relative Role Of Trust And Control*, 25 J. ECON. PSYCHOL. 243, 259 (2004). *See also* F. Stutzman et al., *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIVACY & CONFIDENTIALITY 2, 29 (2013) (finding that as Facebook gave users more control over settings that determine which other Facebook users can view their pages, users made more content "private" vis-a-vis other users, but also posted more confidential information, such that Facebook and parties to which it provides data obtained more information about users).

them to both reveal more sensitive information and to allow more publication of that information.[77] Firms today emphasize the degree to which consumers have control over tracking to encourage consumers to share more information. Google, for example, suggests that consumers connect their accounts (enabling tracking across accounts) because "Connecting your accounts puts you in control" and then reminds consumers, "Remember, Google won't share your searches or other private information with third-party services without your consent."[78] Google itself uses information it gathers about consumers without explicit consent, but the "you are in control" pitch deflects attention from this.[79] Thus, giving consumers the apparent ability to opt out of tracking today may, by giving consumers the illusion of control, make them less likely to attempt to opt out.[80]

h. The sunk costs fallacy refers to a common error—people usually weigh costs they have already incurred and that cannot be reversed in their decision about whether to move forward with a project or switch course.[81] For example, someone who has spent time and effort determining how to use a particular type of software might continue using that software instead of switching to an easier-to-use program because otherwise the effort on the first software seems to have been wasted. But because that time and effort can never be recovered, it should not come into the calculus about what software to use going forwards. Where the option to opt out of a default is not presented until after people have taken some investment in reliance on the default, the sunk costs fallacy will favor the default.

For example, this fallacy may favor the Track-Me position for mobile apps. Consumers must select an app and go through part of the download process before they can learn how much data the app will gather from them if they complete the installation process.[82] At that point, the fallacy may encourage consumers to complete the download process regardless of what data is collected.

77 Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, SOCIAL PSYCHOLOGICAL AND PERSONALITY SCIENCE 3 (2012).

78 GOOGLE PROFILE PAGE, https://profiles.google.com/u/0/connectedaccounts?partnerid=gplp0 (last visited __).

79 *See* Tate, *supra* note __ (reporting on "obscure checkbox on a buried Google account preferences pane, which reads, 'use my Google contact information to suggest accounts from other sites.'" and explaining "[b]y default, this box is checked, which means Google has been scanning your Gmail contacts, unless by some miracle you found this option, buried several clicks beyond your Gmail inbox, and disabled it.").

80 Consumers who take more steps to avoid online tracking today also reveal more about themselves online. Rainie, supra note __ at 18. Although the direction of causation is unknowable, it is possible that the illusion of control contributes to increased disclosure.

81 Hal R. Arkes & Catherine Blumer, *The Psychology of Sunk Cost*, 35 ORG. BEHAV. & HUM. DECISION PROCESSES 124 (1985).

82 *See* Felt et al., *supra* note 39.

3. Preference-Formation Effects

The third type of mechanism through which defaults garner adherents is that involved in the formation of preferences.[83] This happens in two ways, through (a) the recommendation effect and (b) the experience effect.

a. The recommendation effect is the common interpretation of a default as a form of implicit advice by a more knowledgeable party as to what most people prefer or ought to prefer. Where consumers lack pre-existing preferences, they will often follow this implicit advice.[84]

Research demonstrates that consumers follow the crowd, changing their privacy behaviors to match the perceived behaviors of others.[85] When consumers believe tracking defaults are selected based on majoritarian preferences, they may accept them on the basis that they reflect social norms.[86] Alternatively, consumers may select the default because they trust the firms with which they do business (e.g., frequented websites, wireless providers) and assume these firms have set the default with the consumers' best interests in mind.[87]

b. Where people do not have a pre-existing preference, *the experience effect* may lead them to develop a preference for and stick with the default position after spending some time experiencing it. For example, cellphone users who perceive themselves as benefitting from their existing privacy settings might choose to stick with a phone's Track-Me position. Yet, if Do-Not-Track had been the phone's default setting, they would have become accustomed to that position and developed a preference for it instead.[88]

B. CONSUMER HETEROGENEITY AND THE CONDITIONS UNDER WHICH THE MECHANISMS THAT MAKE DEFAULTS STICKY OPERATE

Not all of the mechanisms that can make defaults sticky operate on all consumers all the time. One source of heterogeneity is differences in consumer susceptibility to biases. For example, consumers approach choices with different discount functions, not all consumers are affected by omission bias, and while most of us are procrastinators, consumers do not all procrastinate on the

83 *See, e.g.*, Cass Sunstein, *Switching the Default Rule*, 77 N.Y.U. L. REV. 106 (2002), (discussing preference-formation effects of defaults).

84 *See, e.g.*, Craig R. M. McKenzie et al., *Recommendations Implicit in Policy Defaults*, 17 PSYCH. SCI. 414, 414 (2006).

85 Alessandro Acquisti et al., *The Impact of Relative Judgments on Concern about Privacy*, 49 J. MKTG. RES. 3 (2012),

86 *See, e.g.*, Tene & Polonetsy, *supra* note **Error! Bookmark not defined.**, at 341; Janger & Schwartz, *supra* note **Error! Bookmark not defined.**, at 1250 (explaining that information privacy norms are shaped by existing information privacy practices).

87 Although cellphone companies do not fare as well, Amazon, Google, and Apple are among the ten companies with the highest reputations among consumers, and trust is one of the major drivers of these ratings. Harris Poll 2013 Reputation Quotient Survey Summary Report 6 & 9, HARRIS POLL (Feb. 2013), http://www.harrisinteractive.com/vault/2013%20RQ%20Summary%20Report%20FINAL.pdf.

88 *Cf.* Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010 (2013) (suggesting that reactive nature of U.S. privacy policymaking leads to less privacy protection because social norms adjust to the status quo).

same things or to the same extent.[89] Consumer responses to transaction barriers are also heterogeneous, independent of consumer valuations of the default and opt-out positions; for example, some consumers might find an opt-out process confusing that others have no trouble completing. Much of this heterogeneity does not correspond well to who ought to opt out and who ought to stick with the default. Whether someone suffers from the illusion of control or is more realistic in her appraisal, for example, might affect whether she opts out of a risky default position, but may not be a good barometer of whether she ought to take on the risky or less risky position.

Two sources of heterogeneity, however, are theoretically well-aligned with the use of defaults that aim to be sticky: consumers' understanding of their options and consumers' understanding of their own preferences. When consumers understand their options and their preferences well, they can usually match the two easily, absent transaction barriers. A consumer who knows she prefers the opt-out position will not be swayed by the implicit advice conveyed in the policymaker's selection of the default, for example.[90] Likewise, consumers who already know their options are unlikely to be affected by how salient each option is at the moment of decision. In these situations, biases and the preference-formation effects of defaults have little influence on outcomes. That is, defaults will not be sticky.[91]

But when consumers do not understand their options, their preferences, or both, the framing of the decision can strongly influence the consumer's choice. When options are numerous, complex, indistinct, shifting, or have uncertain attributes, consumers are routinely unable to evaluate and compare all options. Consumers might find their own preferences opaque when they hold those preferences weakly, have had insufficient experience to form preferences, and/or have competing preferences involving incommensurate tradeoffs. Under these conditions, the option framed as the default will often be sticky.[92] This is not the direct result of the option being presented as the default. It is because many of the mechanisms that make defaults sticky are more likely to operate when consumers find the decision environment or their own preferences opaque.[93]

89 Cite (finding discount functions vary); Jonathan Baron & Ilana Ritov, *Omission Bias, Individual Differences, and Normality*, 94 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 74, 74 (2004) (finding that not everyone is affected by the omission bias, and some even display an action bias); cite (finding procrastination varies).

90 *Cf.* Erin Todd Bronchetti et al., *When A Nudge Isn't Enough: Defaults And Saving Among Low-Income Tax Filers*, NBER Working Paper 16887 (2011), http://www.nber.org/papers/w16887 (finding that placing part of tax refund in a savings vehicle by default had no effect on whether taxpayer saved the funds, and suggesting that the result was because taxpayers had well-understood pre-existing preferences about whether to save or spend the funds).

91 *See, e.g.*, Korobkin, *supra* note 60, at 1622 (presenting evidence that when preference uncertainty is removed, defaults lose their power).

92 *See, e.g.*, Samuelson & Zeckhauser, *supra* note 59, at 29 (finding that choice difficulty increases the pull of defaults); *id.* at 8 (finding subjects more likely to choose to remain with the status quo when their preferences are weaker).

93 Sarah Lichtenstein & Paul Slovic, *The Construction of Preference: An Overview*, *in* THE CONSTRUCTION OF PREFERENCE 1 (Sarah Lichtenstein & Paul Slovic eds., 2006) (observing that judgment and decision biases are strongest when preferences are uncertain). Other academics have described this process a bit differently, claiming that when consumers lack pre-existing preferences, they construct preferences in the course of decisionmaking, and that the framing of the decision through the presence of a default shapes how that preference is constructed. But a position's status as a default does not alone drive consumers towards that position; rather, the mechanisms that can make defaults sticky must come

Most consumers understand their information privacy options poorly.[94] The variety of data that can be collected through tracking, the host of entities that can collect or obtain that data, the ways that data can be used, and the potential costs and benefits of data collection are bewildering. The intangible effects of tracking are nigh impossible to assess; for example, most people probably cannot forecast whether any particular tracking will make them feel watched or how such a feeling will impact their lives.[95] Even as to concrete effects, people do not know—and cannot know--what effect their data will have on prices they pay, access to employment, chances of identity theft, and so on.[96] This complexity defies simplification. As one set of researchers who found that simplifying the language and formatting of privacy policies barely improved consumer comprehension put it: "[E]ven the most readable policies are too difficult for most people to understand and even the best policies are confusing."[97]

Most consumers have a similarly poor grasp of their own privacy preferences and of what actions are necessary to meet those preferencesIn part this may be because technology is evolving so rapidly that they have not thought about who has access to their data and how it might be used.[98] Even consumers who describe themselves as placing a very high value on privacy act in ways that reveal abundant private information; most consumers who say they want to keep information about themselves private will reveal that very information when asked for it, even when asked by a computer "bot" (interactive figure) on a commercial website.[99] Consumers also have competing preferences and cannot make the tradeoffs between the incommensurate costs and benefits of privacy; they want to keep their personal information private *and* they want the benefits made

into play. *See* Julie R. Agnew et al., *Who Chooses Annuities? An Experimental Investigation of the Role of Gender, Framing and Defaults*, 98 AM. ECON. REV. 418, 421 (2008) (finding experimentally that defaults have no effect when transaction barriers, biases, and preference formation effects are absent). Further, many of these mechanisms can lead a consumer to remain in a default position without affecting her preferences; a consumer who sticks with a default due to transaction costs or salience effects does not necessarily prefer the default over the opt-out position, ceterus paribus.

94 *Cf.* Jensen et al., *supra* note **Error! Bookmark not defined.** (finding that consumers have little understanding of even well-publicized privacy-related technologies, such as cookies).

95 *See, e.g.*, Ur et al.,*supra* note __ ; Aleecia M. McDonald & Lorrie Faith Cranor, *An Empirical Study of How People Perceive Online Behavioral Advertising*, (Carnegie Mellon Univ., Working Paper, Nov. 10, 2009), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09015.pdf.

96 *See* Acquisti & Grossklags, *supra* note 66.

97 Aleecia M. McDonald et al., *A Comparative Study of Online Privacy Policies and Formats*, 5672 LECTURE NOTES IN COMPUTER SCI. 37, 52 (2009).

98 *Cf.* Chris Jay Hoofnagle et al., *Privacy and Modern Advertising: Most US Internet Users Want "Do Not Track" to Stop Collection of Data About their Online Activities* 10 (Oct. 8, 2012), http://goodtimesweb.org/documentation/SSRN-id2152135.pdf (finding that 87% of consumers had never heard that policymakers are considering a "Do Not Track" option for the internet).

99 *See* Sarah Spiekermann et al., *E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior* § 3.3 (2002), http://people.ischool.berkeley.edu/~jensg/research/paper/grossklags_e-Privacy.pdf.

possible by revealing that information.[100] One survey's findings are telling: 84% of consumers say they would rather receive targeted advertising in exchange for online content than to pay for online content with money, but 93% of these same consumers say that they would opt into a Do-Not-Track position if given the choice.[101]

Thus, the personal data tracking area seems to be one in which consumer uncertainty about options and their own preferences would facilitate the operation of mechanisms that make defaults sticky.[102]

C. THE THEORY BEHIND THE USE OF DEFAULTS IN POLICYMAKING

Observing that people tend to stick with many default settings, academics have suggested that defaults can be used in policymaking in two ways: to increase the number of people in the default position (policy defaults) or to provide private parties with incentives to educate people about the default (penalty defaults). To ensure that policy defaults are sticky for consumers with weak preferences but not for those who prefer the opt-out position, and to ensure that penalty defaults are information-forcing, policymakers have sought to employ a variety of altering rules (rules about the process for opting out) and framing rules (rules about the presentation of the default). The following explains the theory behind (a) policy defaults, (b) penalty defaults, and (c) altering and framing rules.

a. *Policy defaults* are put in place with the explicit goal of increasing the number of people in the default position.[103] The idea is to set the default to a position that is good for most individuals and/or for society,[104] under the assumptions that (1) the majority will stick with the default and (2) the minority who have contrary preferences, and only this minority, will opt out. The use of policy defaults theoretically aligns well with the fact that the mechanisms that make defaults sticky are more likely to operate where consumers are uncertain about their preferences and options. The default will in theory guide uncertain individuals to the position that is most likely to be the best for them, but will not prevent those who know they have contrary preferences from opting out.

The iconic case of a policy default is automatic enrollment in defined contribution retirement savings plans, which is believed to be the best position for the vast majority of employees. Employers that have made participation in their plans the default have increased their employee

100 *See, e.g.*, Patricia A. Norberg et al., *The Privacy Paradox: Personal Information Disclosure Intentions versus Behavior*, 41 J. CONSUMER AFFS. 100 (2007); James P. Nehf, *Shopping for Privacy on the Internet*, 41 J. CONSUMER AFFS. 351, 359 (2007); Blasé Ur et al., *supra* note at 6 (explaining that consumers find tracking for advertising purposes scary and creepy yet also smart and useful).

101 *Internet Users' Response to Consumer Online Privacy*, *supra* note **Error! Bookmark not defined.**.

102 *Cf.* Eric J. Johnson et al., *Defaults, Framing and Privacy: Why Opting In ≠ Opting Out*, 13 MARKETING LETTERS 5 (2002) (finding large default effect in a privacy-related experiment, and suggesting that people's uncertainty about their preferences contributes to the power of privacy defaults).

103 *Accord* McKenzie et al., *supra* note 84, at 414.

104 *See also* Janger & Schwartz, *supra* note **Error! Bookmark not defined.**, at 1236, 1245–46 (using "majoritarian defaults" to refer to default positions set to what the policymaker believes the majority of relevant parties would want and "normative defaults" to refer to default positions set to what the policymaker believes is best for society).

participation rates by forty percentage points or more.[105] Another example is the default for checking account overdraft coverage, which effectively requires banks to default consumers out of expensive overdraft coverage for ATM and nonrecurring debit card transactions unless the consumer opts out.[106] Regulators enacted this default in part on the theory that the default position was the best position for most consumers, and the few consumers who benefitted from overdraft coverage on these transactions could opt out.[107]

b. *Penalty defaults* are used to correct information asymmetries between parties, such as commonly exists between firms and consumers. The default is set to a position disliked by firms, on the premises that firms that want consumers to opt out will be forced to (1) reveal the default and (2) engage in a process of negotiation.[108] Like policy defaults, penalty defaults align well with the evidence that uncertain consumers are more likely to be affected by the default. Firm efforts to explain the default and opt-out positions so as to convince consumers to opt out will, in theory, educate precisely those consumers who need to know more about the default to make a good decision.

Two well-known penalty defaults are the warranties of merchantability109 and of fitness for a particular purpose110 under the Uniform Commercial Code. The penalty default is that the warranties will apply; a seller that does not want the warranties to be part of the contract for sale must explicitly opt out.111 The checking account overdraft coverage default can also be seen as penalty default, on the theory that if the bank wants consumers to opt out, it will be forced to explain how overdraft coverage works and convince consumers to opt out of the default and into overdraft coverage.

c. Policymakers attempt to manage the stickiness, slipperiness, and informativeness of defaults through *altering rules and framing rules*. Altering rules tinker with the process for opting out. For example, a software default setting can be designed to allow a user to opt out with a single click, or can require a user to go through many steps. Framing rules manage the way the default and opt-out option are presented to the user, whether by architecture or by messaging. Architecturally, for example, a software default setting could be made more or less salient through the positioning of opt-out controls, hidden deep inside multiple menus or popping up in a nagging window on the screen. Opting out of a default also might be made more or less attractive through messages

105 *See, e.g.*, William E. Nessmith et al., *Measuring the Effectiveness of Automatic Enrollment*, 31 VANGUARD CTR. FOR RETIREMENT RES. RPT. 6 (2007).

106

107

108 *See* Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 91 (1989); *see also* Janger & Schwartz, *supra* note **Error! Bookmark not defined.**, at 1239 (dubbing penalty defaults "information-forcing defaults").

109 UCC § 2-314.

110 UCC § 2-315.

111 UCC 2-316. Note that in the consumer context, the Magnusson Moss Act restricts the degree to which these default warranties can be disclaimed.

conveyed to the user. For example, an alert or notice box might suggest that the user ought to change a software setting, or instead warn the user that changing the setting could result in problems.

Where a default might otherwise be too sticky, altering rules might aim to keep the costs of opting out low and the process for opting out simple and framing rules might aim to keep the option to opt out visible. But where policymakers fear a default will be too slippery and will not be information-forcing, they might set altering rules that place some transaction costs in the way of opting out and framing rules that require the provision of information as a precondition of opting out. Altering and framing rules reflect some awareness that defaults alone will not achieve their desired ends. A default otherwise might be stickier than the policymaker intends, such that the minority who ought to opt out do not. Or a default might otherwise be slipperier than a policymaker intends, such that the better-informed party is able to change the default without educating and negotiating with the less-informed party. The theory is that carefully calibrated altering and framing rules will make policy and penalty defaults work properly.[112]

Two examples show how surrounding rules are employed in an attempt to calibrate the stickiness of defaults. In the case of automatic enrollment in retirement savings plans, policymakers are concerned that the default could be too sticky. Altering and framing rules therefore require employers to give employees who are enrolled by default written notices of the right to opt out at specified intervals, notices that must be written at a level that can be understood by the average employee, so that the opportunity to opt out is not confusing or invisible.[113] In contrast, policymakers are concerned that the default for checking account overdraft coverage on ATM and debit transactions could be too slippery and might not be information-forcing.[114] Therefore, framing rules require banks to give accountholders notices explaining the cost of opting out of the default and into overdraft coverage—notices that must be segregated out from other account documents.[115] Altering rules require banks to provide the same account terms, conditions, and features to

112 Ayres, *supra* note __ at __ (get quote from the Regulating Opting Out article to this effect).

113 IRS Income Tax Rule, 26 C.F.R. § 1.401(k)–3(d)(3) (2004) ("The content requirement . . . is satisfied if the notice is (A) Sufficiently accurate and comprehensive . . . (B) Written in a manner calculated to be understood by the average employee…").

114 Electronic Fund Transfers, 12 C.F.R. § 205.17(b) (2010). An overdraft occurs when an accountholder attempts to withdraw more from her checking account than is available, and the bank covers the withdrawal and then reimburses itself when the next deposit is made into the account. For what amounts to a short-term loan the bank charges the accountholder a fee, one that is frequently larger than the amount borrowed. *See* FED. DEPOSIT INSURANCE CORP., FDIC STUDY OF BANK OVERDRAFT PROGRAMS V & 15 (Nov. 2008), http://www.fdic.gov/bank/analytical/overdraft/FDIC138_Report_Final_v508.pdf (finding in a 2007 survey of banks that the median negative balance from a debit transaction on which an overdraft fee was charged was about $20 and the median fee was $27).

115 12 C.F.R. § 205.17(d) (2010).

accountholders who do and do not stick with the default,[116] and prohibit banks from opting consumers out in routinely unread fine print; consumers must affirmatively take action to opt out.[117]

III. TRANSLATING DEFAULT THEORY TO TRACKING POLICY

The rationales for using defaults, the mechanisms that make them sticky, and the background conditions that facilitate the operation of those mechanisms appear to favor the use of defaults in privacy policymaking. Not the illegitimate Track-Me quasi-default that currently exists; if policymakers want consumers to make their own decisions about tracking, consumers ought to be permitted to choose the Do-Not-Track position. But given that many consumers are uncertain about their choices and preferences, policy defaults might help lead these consumers to the best outcome while allowing consumers with contrary preferences to opt out, and penalty defaults might force firms to educate consumers to help consumers make better decisions. The following describes the personal data tracking default positions, the scope of those positions, and the accompanying altering and framing rules that the theory behind the use of defaults in policymaking would support.

A. SETTING: TRACK-ME OR DO-NOT-TRACK

How any particular tracking default ought to be set and how it is expected to function in theory depends on the policymaker's prior beliefs about which position is best for most people. If policymakers believe tracking produces more potential benefits to individuals and society (for example, in the form of financial support for internet content or application development) than potential privacy harms, they might support a Track-Me default. Because in this scenario policymakers believe that the majority ought to be in the Track-Me position,[118] it would be a policy default. For example, the World Wide Web Consortium (W3C), the main international standards-setting body for the internet,[119] has drafted a proposal that would, in effect, set Track-Me as the default for some tracking of some information about individuals' use of the internet and mobile devices.[120] The Federal Trade Commission (FTC) has suggested that a similar Track-Me default

116 12 C.F.R. § 205.17(b)(3) (2010).

117 12 C.F.R. § 205.17(b)(1)(iii) (2010).

118 Policymakers might support a Track-Me default on political expediency or other grounds as well, but this discussion focuses on the tracking default setting that the theory underlying the use of defaults in policymaking would support.

119 See http://www.w3.org/Consortium/ ("The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards."); see also http://en.wikipedia.org/wiki/World_Wide_Web_Consortium.

120 The current draft scheme is described in two documents: WORLD WIDE WEB CONSORTIUM, TRACKING COMPLIANCE AND SCOPE–W3C EDITOR'S DRAFT (June 25, 2013), http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html [hereinafter "W3C Functional Specifications"], and WORLD WIDE WEB CONSORTIUM, TRACKING PREFERENCE EXPRESSION (DNT)—W3C WORKING DRAFT (Apr. 30, 2013), http://www.w3.org/TR/tracking-dnt/ [hereinafter "W3C Technical Specifications"]. The W3C draft default requires general purpose browsers to be initially set to "Track-Me" or "No Preference," either of which would permit tracking. W3C Technical Specifications, at § 3, Determining User Preference, http://www.w3.org/TR/tracking-dnt/. However, a consumer can opt out by using a special-purpose browser that is marketed as a privacy-enhancing technology. *Id.*

should be voluntarily adopted by firms or mandated by Congress for all firms that collect or use consumer data that can reasonably be linked to particular consumers, computers, or devices.[121]

On the other hand, if policymakers believe that tracking produces more potential privacy harms (for example, in the form of increased risk of identity theft or decreased space for individual experimentation and growth) than benefits to individuals and society, they might support a Do-Not-Track default. Because they believe that the untracked position is best for most people or for society, these policymakers would be again looking for a policy default effect, meaning that the majority would stick with this default position but those with strong contrary preferences would opt out. Many supporters of Do-Not-Track defaults appear to aim for a policy default effect.[122]

If policymakers are uncertain about the social welfare effects of tracking or believe that people have heterogeneous preferences about tracking, they also might support a Do-Not-Track default. Personal information tracking presents a case of information asymmetry, where one party (the firm) is well informed and the other (the consumer) is poorly informed. Because many internet and mobile application firm business models depend on the revenue that can be obtained through the sale of tracked information (largely for behavioral advertising purposes), firms have a strong interest in placing consumers in a Track-Me position.[123] Thus, a policymaker might intend for the Do-Not-Track default to operate as a penalty default, with the expectation that firms will reveal this default position to consumers in the process of urging consumers to opt out, and that consumers will then be free to make informed decisions about whether they want to be tracked. Academics in particular have argued for various forms of Do-Not-Track defaults on this basis.[124]

---

121 See FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE vii & 35-59 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter, FTC Privacy Report]. *See also* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES 21(Feb. 2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf [hereinafter, FTC Mobile Privacy Report].

122 *See, e.g.*, Chris Soghoian, *End The Charade: Regulators Must Protect Users' Privacy By Default*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (Dec. 2010), http://www.priv.gc.ca/information/research-recherche/2010/soghoian_201012_e.asp (implying that a Do-Not-Track default would be so sticky that advertisers would be forced to abandon behavioral advertising); Tene & Polonetsky, *supra* note **Error! Bookmark not defined.** (suggesting that supporters of Do-Not-Track defaults aim to keep people in the Do-Not-Track position rather than to give people a choice).

123 *See, e.g.,* Vindu Goel, *Facebook Eases Privacy Rules for Teenagers*, N.Y. TIMES, Oct. 16, 2013 ("But fundamentally, Facebook wants to encourage more public sharing, not less. The company, which has about its 1.2 billion users worldwide, is locked in a battle with Twitter and Google to attract consumer advertisers like food, phone and clothing companies."); James Temple, *Rules Against Tracking Don't Go Far Enough*, SAN FRANCISCO CHRONICLE, Mar. 7, 2012, available at http://www.sfgate.com/business/article/Rules-against-online-tracking-don-t-go-far-enough-3387373.php ("Targeting ads based on search queries, sites visited, stories read and social connections forms the core of the multimillion-dollar business models of many online companies, including Google, Yahoo and Facebook.").

124 *See, e.g.*, Kesan & Shah, *supra* note 13, at 621 (arguing that setting browser defaults to reject cookies "would ensure that people understood the privacy risks of cookies"); Paul M. Schwartz , *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2100 (2004) ("This Article prefers an opt-in default because . . . it would place pressure on the better-informed party to disclose material information about how personal data will be used. This default promises to force the disclosure of hidden information about data-processing practices.").

B. SCOPE AND GRANULARITY OF DEFAULT AND AVAILABLE OPT-OUT POSITIONS

When setting a default position, policymakers must also consider the issue of scope, both as to the initial default and as to the available opt-out position or positions. The costs and benefits of tracking might vary for different types of information collected (e.g., geolocation data, clickstream data,[125] medical data, email content), uses of information (e.g., medical research, marketing, pricing, website use analytics, employment), collection sites (e.g., particular websites, mobile applications), types of users of information (e.g., first-party entities with which consumers intend to interact, affiliates of first-parties, third-parties to which first-parties sell data or access to data[126]), and individual users (particular firms or other entities).[127] The default could be set broadly to Track-Me (or Do-Not-Track) for most types, uses, collection sites, user types, and individual users of information, or a mix of narrower defaults and unalterable positions could be employed. Where a position is a default, the policymaker must further consider whether a consumer can or must be given the opportunity to opt out broadly or selectively, again along any of these dimensions.

Consider the policymaker's decision about whether to require firms to give consumers choice, or to set (or allow firms to set) an unalterable position. For some information, policymakers might decide that the benefits of tracking are outweighed by costs, regardless of consumer preferences, and therefore set an unalterable Do-Not-Track position for that information. For example, tracking of sexual orientation or medical data for employment purposes could be generally prohibited. For other data, policymakers might decide that the benefits of tracking strongly outweigh any costs, and thus set an unalterable Track-Me position. For example, firms might be permitted to track clickstream data for website analytics purposes, without giving consumers an ability to opt out.

Despite the overarching policymaker goal of individual personal data privacy choice, no proposal to date appears to contemplate giving consumers complete control over tracking. Instead, all proposals retain some categories of information tracking from which consumers cannot opt out. For example, the current W3C's draft proposal would allow consumers to opt out of tracking only with respect to certain data collected by third parties for certain purposes, such as behavioral advertising, and geolocation data more granular than the zip code level collected by third parties for any purpose. First parties can continue to collect any and all data and can customize content and advertising based on the consumer's interaction with that firm.[128] Third parties can continue to

125 Clickstream data refers to the information generated by users' mouse movements and clicks through the website they visit, as well as the sites visited, duration of the visit and order of site visits. *Definition: Clickstream Analysis*, SEARCHCRM, http://searchcrm.techtarget.com/definition/clickstream-analysis (last visited Aug. 1, 2013).

126 But given that third parties can become affiliates of first parties and that first parties can act as the handmaidens of third parties, tracking defaults that turn on these distinctions may be subverted. *Cf.* Mitch Weinstein, *Why Blocking Third-Party Cookies Is Good for Google and Facebook*, ADEXCHANGER (June 20, 2013), http://www.adexchanger.com/data-driven-thinking/why-blocking-third-party-cookies-is-good-for-google-and-facebook/.

127 The original collection of data can be regulated, and/or downstream users or uses can be regulated. Enforcement concerns would push toward limiting the original collection of data, even where only some potential downstream users or uses are problematic. However, to present the strongest case for the use of tracking defaults, this article sets aside these enforcement concerns. See supra note __.

128 W3C Functional Specifications, at § 4, First-Party Compliance.

collect data for "permitted purposes," including frequency capping (measuring how many times a consumer has been shown an ad), billing (to ensure third-party advertisers are paying first-party websites correctly), and debugging, and can continue to collect gross geolocation data for any purpose.[129] Consumers cannot opt out of any tracking by first parties, tracking of gross geolocation data by any party, or tracking for "permissible purposes" by third parties. Similarly, the FTC tracking proposal allows first parties to collect and use information about consumers without giving consumers an opportunity to opt out where "the practice [of data collection and use] is consistent with the context of the transaction or the consumer's existing relationship with the business, or is required or specifically authorized by law."[130] Contextually-appropriate uses not requiring consumer choice would include the collection and use of data for the purposes of "fulfillment, fraud prevention, internal operations, legal compliance and public purpose, and most first-party marketing."[131] These types of limitations on the extent to which consumers can control tracking may be necessary to avoid giving consumers the impression they must accept all tracking in order to receive a benefit that most consumers want, such as for their orders to be filled or fraud prevention. However, allowing consumers to opt out of some but not all tracking could also be confusing and lead to a sense that opting out is futile.

Within the set of potentially tracked information about which policymakers wish to give consumers control, policymakers then must decide which defaults should be Track-Me and which should be Do-Not-Track. For example, the FTC has suggested that the default for sensitive information--"information about children, financial and health information, Social Security numbers, and precise geolocation data"--should be Do-Not-Track, thus requiring express consent from consumers before the information can be collected.[132] The proposed default for the collection of nonsensitive information by third parties (or affiliates of first parties where the affiliate relationship is not obvious to consumers) or by first parties tracking consumers across third-party websites, or for first parties sharing nonsensitive information with third parties, would be Track-Me.[133] Thus, for example, first parties would need to obtain consumer consent before collecting sensitive data and would need to give consumers an opportunity to opt out of sharing nonsensitive data with third parties.

Once policymakers decide to allow consumers to opt out of a particular type of information tracking, they then must decide the scope of the opt-out mechanism. Opting out of a default wholesale might be the only alternative given to consumers, or consumers might be permitted to opt out narrowly. For example, a consumer might be given the power to opt out of a Track-Me or Do-Not-Track default as to third parties while continuing to be tracked by first parties, and/or to opt out on a firm-by-firm basis. To the extent that tracking is performed through cookie technology,

129 *Id.* at § 5, Third-Party Compliance.

130 FTC Privacy Report, *supra* note __ at 38-39.

131 *Id.* at 39.

132 FTC Privacy Report at 59.

133 *Id.* at 40-42.

common web browser setting choices today give consumers the ability to opt out on both of these bases. For example, in Firefox today, a consumer can choose to accept no cookies, accept cookies from first parties but not third parties, accept all cookies, and/or make exceptions from each of these for particular websites.[134]

The broader the tracking default setting and opt-out mechanism, the more easily it is understood by consumers, but the more likely that consumers will be unable to satisfy their textured preferences. For example, a Do-Not-Track default setting that prohibits all passive personal data collection is intuitive, but most consumers want some tracking for some purposes (e.g., geolocational tracking to locate a lost or stolen mobile device, clickstream data tracking for the purposes of pre- or re-populating online forms). A scheme of narrow defaults, such as a different setting for each potential use or user of each potential type of data, or a broad default with a granular set of selective opt-out options, would allow sophisticated consumers to satisfy particular preferences, but presents the danger of overwhelming the average consumer.[135]

Given that the overarching goal of the use of personal data defaults is to facilitate individual choice about whether, when, and by whom to be tracked, it seems likely that policymakers will create a scheme by which consumers can selectively opt in or out of tracking defaults. Unsurprisingly, most tracking default proposals permit consumers to, in effect, opt out on a firm-by-firm basis. Regarding tracking of mobile devices, the FTC has suggested that the default for some information be Track-Me, that consumers be permitted to opt out from this wholesale, but that consumers then be permitted to opt back into tracking on an application-by-application basis:

> A DNT setting placed at the platform level could give consumers … a way to control the transmission of information to third parties as consumers are using apps on their mobile devices. …Offering this setting or control through the platform will allow consumers to make a one-time selection rather than having to make decisions on an app-by-app basis. Apps that wish to offer services to consumers that are supported by behavioral advertising would remain free to engage potential customers in a dialogue to explain the value of behavioral tracking and obtain consent to engage in such tracking.[136]

The W3C proposal is similar. To the extent that it gives consumers control over tracking, it effectively sets Track-Me as the default and requires that the option to opt out be made available to consumers at the browser level.[137] Consumers who select the Do-Not-Track position at the browser level would then be permitted to opt back into the Track-Me position wholesale or selectively.[138] If

134 Go to Firefox, Options, Privacy. As previously noted, however, trackers can track through other means than cookies, such as through digital fingerprinting. See Cookie has 5 years to live, supra, and fingerprinting source, supra.

135 For example, when Facebook added more granular privacy controls, users became confused and were more likely to stick with default settings. *See* Stutzman et al., *supra* note 76, at 23.

136 FTC Mobile Report at 21.

137 W3C Technical Specifications, at § 6, User Granted Exceptions.

138 W3C Technical Specifications, at § 6, User Granted Exceptions.

the default were Do-Not-Track, a comparable scheme might be to give consumers both a wholesale opt-out choice, allowing them to opt into the Track-Me position with respect to all firms, and a granular choice, allowing them to opt out on a firm-by-firm basis.

C. ALTERING AND FRAMING RULES

Policymakers would then need to select framing and altering rules for these defaults. Recall that the goals of such rules are to prevent the default from being too sticky or too slippery and to inform consumers about the default and opting out. Given that the tracking defaults and opt-out choices policymakers appear likely to embrace are complex, ensuring that consumers understand their choices and are able to act on them is likely to be a demanding task. While the theoretically possible altering and framing rules are limitless, this section sketches the general contours of the rules policymakers are likely to select.

First, policymakers are likely to put rules in place that aim to make the default and opportunity to opt out visible and perhaps even salient. For example, rules might require the default and opportunity to opt out to be "prominent"[139]--disclosed in words that "are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear"[140] The FTC proposal suggests that the choice to be opt out must be given to consumers "at a time and in a context relevant to the consumer's decision about whether to allow data collection and use," such as "directly adjacent to where the consumer is entering his or her data [online]," "immediately upon signing up for a service," or, for on offline transaction, "close to the time of sale" through notification on a "sales receipt" or "prominent poster at the location where the transaction takes place."[141]

Second, to forestall the confusion that can make defaults overly sticky, policymakers are likely to require that the mechanism for opting out be "easy to find and use."[142] More particularly, firms might be required to create an opt-out process that involves no more than one or two clicks of a tangible or virtual button to opt out.[143] The opt-out process might be standardized, at least to some extent, across browsers, websites, mobile devices, or applications. Or the process for opting back into the default after having opted out might be regulated so that firms could not change a consumer's position through unread fine print. For example, while the W3C default scheme does not contain rules regarding the process for opting out of the default,[144] it does require that where a

139 *See* FTC Privacy Report at 50. See also In the Matter of ScanScout, Inc., FTC Fo. 102 3185 (2011) (Consent Order), http://www.ftc.gov/os/caselist/1023185/111221scanscoutdo.pdf [hereinafter "ScanScout consent order"] (requiring "prominent" placement of a notification about a default and opt-out mechanism).

140 ScanScout consent order.

141 FTC Privacy Report at 50.

142 *See* FTC Mobile Report at __.

143 *See* ScanScout consent order.

144 *See* W3C Technical Specifications, at § 3, Determining User Preference ("We do not specify how tracking preference choices are offered to the user or how the preference is enabled: each implementation is responsible for determining the user experience by which a tracking preference is enabled. For example, a user might select a check-box in their user

consumer has opted out at the browser level, opting back in to a Track Me position with respect to any particular firm must be done "explicit[ly]."[145]

Rules aimed at visibility and eliminating confusion would simultaneously work to inform consumers about the default and opt-out opportunity. For example, the W3C default scheme requires firms that track consumers and all browsers to "clearly and accurately" with a "brief and neutral explanatory text" explain that a consumer can opt out of some third-party tracking, that a consumer who has opted out may continue to be tracked for "permissible" purposes, and that a consumer who has opted out at the browser level can opt back in with respect to a particular firm.[146] Where a consumer has opted out of tracking at the browser level, the consumer's opting back in selectively must be "informed."[147]

Third, policymakers might put rules in place intended to minimize the costs of opting out. For example, rules might require that consumers be given a "universal" opt-out mechanism at the browser or device level, such that opting out once opts the consumer out of all tracking by websites viewed with that browser or applications used on that mobile device.[148] A universal mechanism would also present consumers with a broadly-bracketed choice, perhaps leading to more privacy-minded decisions. To keep the cost of opting out low, rules might require the opt-out mechanism be "persistent,"[149] meaning that firms could not require consumers to opt out repeatedly the way that cookie-based opt-out systems do today.

In theory, a Track-Me or Do-Not-Track default might also prohibit firms from giving consumers incentives to agree to tracking. The law might require firms to treat consumers in the Do-Not-Track position the same as consumers in the Track-Me position, other than as to the particular purposes for which the firm tracks consumers. However, when the existence of the content and features of a website or app currently depends on revenue generated by tracking, policymakers are unlikely to want to undermine this arrangement. The W3C default scheme explicitly permits firms to condition services on consumers agreeing to be tracked, either by staying in the Track-Me default position or by explicitly consenting to tracking by that firm, for just this

agent's configuration, install an extension or add-on that is specifically designed to add a tracking preference expression, or make a choice for privacy that then implicitly includes a tracking preference (e.g., Privacy settings: high). The user-agent might ask the user for their preference during startup, perhaps on first use or after an update adds the tracking protection feature. Likewise, a user might install or configure a proxy to add the expression to their own outgoing requests.")

145 W3C Functional Specifications, at § 6, User Granted Exceptions

146 W3C Functional Specifications, at § 3, User Agent Compliance.

147 W3C Functional Specifications, at § 6, User Granted Exceptions.

148 *See* FTC Mobile Report at __ (suggesting a universal mechanism to opt out of the Track-Me default be made available at the mobile device level).

149 *See* FTC Mobile Report at __.

reason.[150] With a narrow exception for "important product[s] with few substitutes, such as a patented medical device," the FTC proposal also asserts that firms should be permitted to condition goods, services, website content, etc. on consumers agreeing to tracking and to offer tracked consumers lower prices or other benefits.[151]

Moreover, if differential treatment beyond perks incident to the purposes for which the firm tracks consumers were prohibited, the line between these perks and those that cross the line into incentives to agree to tracking could be difficult to police. Firms could provide consumers who agreed to be tracked with many perks that are arguably incident to the "purposes" for which the consumers are being tracked. For example, apps or websites could be optimized for functioning when tracking is enabled. A search engine might display websites in the consumer's language automatically only if the consumer consents to tracking.[152] Or a website might deliver consumers who consent to tracking behaviorally targeted ads and serve untracked consumers a larger quantity of contextual ads. Detecting when the larger quantity is necessary to produce revenue equivalent to behavioral ads and when it is harassment to induce consumers to agree to tracking might not be possible. Thus, even if altering rules prohibited the use of perks or differential treatment to give consumers an incentive to agree to tracking, enforcing this prohibition would likely prove impossible.

V. DEFAULTS IN PRACTICE

Defaults in practice do not always live up to the theory behind using defaults in policymaking. This Part describes two failed default schemes, demonstrates how firms have frustrated these schemes by making the defaults too sticky or too slippery, and, through comparison to examples of relatively successful defaults, extracts a set of conditions under which defaults do not perform in accordance with theory.

A. TWO FAILED DEFAULT SCHEMES

Two failed default schemes are the defaults (a) for the sharing and use of consumer information by financial institutions and (b) for bank overdraft programs. The former is excessively sticky, and the latter is too slippery. Neither appear to lead to well-informed consumer decisions about whether to stick with the default or opt out.[153]

150 W3C Technical Specifications at § 1, Introduction ("Web sites that are unwilling or unable to offer content without such targeted advertising or data collection need a mechanism to indicate those requirements to the user and allow them (or their user agent) to make an individual choice regarding exceptions.").

151 FTC Privacy Report at 52.

152 *Cf. Privacy Policy*, GOOGLE, http://www.google.com/policies/privacy/ (last modified June 24, 2013) ("However, it's important to remember that many of our services may not function properly if your cookies are disabled. For example, we may not remember your language preferences.").

153 By other metrics, these defaults may have done some good. For example, they may have led more financial institutions to share less consumer information or more banks to stop charging overdraft fees than would otherwise have occurred. *See* Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 101 (2002)

a. Financial information defaults: By default, financial institutions collect, use, and share information about their customers for marketing, pricing, and other purposes. Under federal law, consumers can opt out of this in three respects. First, they can opt out to prevent an institution from sharing their personal information with parties that are not affiliated with the institution.[154] Second, they can refuse to permit an institution to share with its affiliates information about the consumer other than information about the institution's own transactions with the consumer.[155] Third, they can opt out of the use by an institution's affiliates of transaction and "other" information for marketing purposes.[156] Even if a consumer has opted out to the fullest extent, financial institutions can share all information with joint marketing partners, transaction information with affiliates for non-marketing purposes, and "as [further] permitted by law."[157]

The defaults are surrounded by altering and framing rules intended to inform consumers and to allow those consumers who prefer to opt out to do so. Institutions must allow consumers to opt out at any time and must provide consumers with a "reasonable means" to do so.[158] A toll-free telephone number or a detachable form with a check-off box is a "reasonable means"; requiring the consumer to write a letter is not.[159] Institutions must give consumers initial and annual notices explaining their opt-out rights.[160] These notices must be "clear and conspicuous," meaning "reasonably understandable" (in plain language and easy to read) and "designed to call attention to the nature and significance of the information" (distinctive in appearance and, if online, located either on a website page that consumers use often or hyperlinked directly from a page where transactions are conducted).[161]

But despite these rules, the financial information defaults appear to be too sticky and are not information-forcing. Consumers reviewing model explanatory notices in laboratory conditions poorly understand the defaults and opt-out provisions.[162] Comprehension is likely to be even lower under real-world conditions, in which many consumers will not read the notices. Further, although

(making this argument as to the financial information defaults). But by the metric of well-informed consumer decisions, the ostensible goal of policymakers, they have failed.

154 Privacy of Consumer Financial Information, 16 C.F.R. § 313 (2000).

155 *Id.*

156 *Id.*

157 16 C.F.R. § 313.15(4).

158 16 C.F.R. § 313.7.

159 *Id.*

160 16 C.F.R. §§ 313.4–5.

161 16 C.F.R. § 313.3.

162 Alan Levy & Manoj Hastak, *Consumer Comprehension of Financial Privacy Notices*, INTERAGENCY NOTICE PROJECT, 9 table 1 (2008), http://ftc.gov/privacy/privacyinitiatives/Levy-Hastak-Report.pdf (showing that less than half the subjects tested were able to select a bank for a cogent and relevant reason based on even the best form notice regulators could develop).

consumers generally do not like banks sharing their information with affiliates or third parties,[163] almost no one opts out.[164]

b. Checking Account Overdraft Default: As explained above, federal banking regulators effectively require banks to default consumers out of bank-funded overdraft coverage for ATM and nonrecurring debit card transactions.[165] Regulators consciously supported the overdraft default with rules intended to prevent bank "circumvention or evasion" of the default.[166] First, to prevent banks from placing language opting out of the default in routinely unread account disclosures, opting out requires an "affirmative" accountholder action, such as speaking to a bank representative in person or by phone or clicking a box on an online banking form.[167] Second, banks must provide the same account terms, conditions, and features to accountholders who stick with the default as they provide to accountholders who opt out.[168] Framing rules require banks to provide consumers with specific information about the default and the consequences of opting out in a document or webpage segregated from all other documents or webpages.[169]

In promulgating the overdraft default, regulators explicitly stated that they intended for it to operate as a policy default, akin to the auto-enrollment default for retirement savings.[170] But it appears that the majority of the consumers whom regulators intended to assist—low-income frequent users of overdraft[171]—opt out of the default.[172] The rule also does not function as a penalty

163 *Id.* at 15 (in consumer testing, finding that respondents "do not seem to like their information being shared with nonaffiliates . . . or affiliates").

164 John Martin, *Opting Out—or Not*, ABCNEWS (June 21, 2001), http://more.abcnews.go.com/sections/wnt/dailynews/privacy_notices_010621.html (finding only .5% of people opt out).

165 Electronic Fund Transfers, 12 C.F.R. § 205.17(b). Fees on bank-covered overdrafts occasioned by other types of transactions (chiefly checks and recurring payments) are not included in the policy default, *see* Supplement I to Part 205, Official Staff Interpretations of 12 CFR § 205.17(b)(2), Comment 2, because these tend to be for necessities and, if not paid, can result in bounced check or late payment fees. ATM and nonrecurring debit transactions tend to be discretionary transactions and when these are declined consumers are not charged a fee. Overdraft Final Rule 2009, *supra* note __, at 59040.

166 Overdraft Final Rule 2009, *supra* note 165(?), at 59044.

167 Requirement for Overdraft Services, 12 C.F.R. § 205.17(b)(1)(iii); 12 C.F.R. Pt. 205, Supp. I, comment 17(b)(1)—4.

168 12 C.F.R. § 205.17(b)(3).

169 12 C.F.R. § 205.17(b)(3).

170 Regulators noted that "studies have suggested [that] consumers are likely to adhere to the established default rule, that is, the outcome that would apply if the consumer takes no action" and cited studies of the effectiveness of automatic enrollment in increasing participation in retirement savings plans. Overdraft Final Rule 2009, 59038 & n. 25.

171 In 2009, one widely-cited industry consultant estimated that 90% of overdraft fees were paid by the poorest 10% of checking accountholders. *See* Editorial, *Debit Card Trap*, N.Y. TIMES (Aug. 20, 2009) (citing Michael Moebs).

172 *See* Willis, *supra* note 34, at __.

default; surveys indicate that consumers who opt out of the default understand it extremely poorly, holding key misconceptions about the way the default and opt-out positions work.[173]

B. HOW FIRMS MAKE THESE DEFAULTS FAIL

Why have these defaults failed? An examination of how these defaults are presented to consumers in practice demonstrates that the mechanisms that sometimes operate to make defaults sticky can be bolstered or undermined. Institutions work to bolster these mechanisms to ensure very few consumers opt out of the financial information default; banks work to undermine these mechanisms to encourage accountholders to opt out of the overdraft coverage default.

a. Transaction Barriers. Transaction barriers that can contribute to the stickiness of defaults—costs, confusion, and futility—can be built higher, eliminated, or even inverted.

In the case of the financial information defaults, institutions prefer for consumers to stay in the default information-sharing position, and therefore build transaction barriers to opting out high. For consumers who attempt to opt out, the altering rule requiring "reasonable means" for opting out keeps the transaction costs of doing so for any one institution fairly low.[174] But consumers must opt out with each financial institution with which they do or have done business. If transaction costs are not enough, institutions warn consumers that opting out will be costly in other ways:

> If you opt out:
>
> We may need you to repeat information that you have already provided and we may not be able to pre-fill applications for you.
>
> We may have to transfer your phone calls more often.
>
> We may not offer you the products that best meet your needs.[175]

Perhaps the largest barrier is invisibility of the option to opt out; even in the flurry of publicity when the notices first went out, fewer than 35% of consumers surveyed recalled receiving

173 *See* CTR. FOR RESPONSIBLE LENDING, BANKS COLLECT OVERDRAFT OPT-INS THROUGH MISLEADING MARKETING, RESEARCH BRIEF 2, 6 n.8 (Apr. 2011), http://www.responsiblelending.org/overdraft-loans/policy-legislation/regulators/CRL-OD-Survey-Brief-final-2-4-25-11.pdf ("Sixty percent (60%) of consumers who opted [out of the default] stated that an important reason they did so was to avoid a fee if their debit card was declined. In fact, declined debit card costs consumers nothing. Sixty-four percent (64%) of consumers who opted [out of the default] stated that an important reason they did so was to avoid bouncing paper checks. The truth is that the opt-in rules cover only debit card and ATM transactions.").

174 The only challenge may be that institutions often require consumers to provide account numbers. *See, e.g.*, *Statutory Form of Opt-Out Notice*, FIRST FOUNDATION, https://www.ff-inc.com/privacy/opt-out-notice.aspx; *Opting Out of Information Sharing*, METLIFE, https://eforms.metlife.com/wcm8/PDFFiles/730.pdf. Locating these might take some time, particularly for closed accounts.

175 *How to Enable Your Cookies*, U.S. AUTOMOBILE ASSOC., https://www.usaa.com/inet/ent_references/CpStaticPages?PAGEID=cp_netprivacy_pub&akredirect=true (last visited Aug. 1, 2013).

them. .[176] Although the law requires that consumers be given initial and annual "conspicuous" notices, these arrive with a heap of other documents from the institution, and this heap is among the reams of disclosures consumers receive, and routinely ignore, in their daily lives.[177] Confusion about the opt-out process and/or about the terms that apply by default also may play a role; as noted above, consumers understand the default and their opt-out rights poorly, even after reading the required notices. That consumers cannot entirely opt out of the sharing of their information with joint marketing partners and affiliates could lead to a sense of futility; a consumer might think "why bother opting out when the institution can still share my data anyway?"

Banks structure the presentation of the overdraft default and the process for opting out to have the opposite effect. Transaction costs do not make the default sticky because banks eliminate these for many consumers, and even make it more costly to stick with the default than to opt out. For new customers and for accountholders using online banking, transaction costs do not fortify the default because these costs are the same whether the consumer sticks with the default or opts out; new accountholders in the process of opening an account or existing accountholders attempting to access online banking must check precisely the same number of boxes regardless of whether they check the box for sticking with the default or for opting out.[178] In addition, some banks flood consumers with marketing encouraging them to opt out, calling them at home or approaching them when they visit a branch.[179] The barrage only ends when the consumer opts out,[180] with the effect that it is costlier to stick with the default—and continue to endure the marketing—than to opt out. Almost half of surveyed consumers who reported that they had opted out of the default did so at least in part to stop receiving overdraft marketing.[181]

Confusion does not make the default sticky, because banks ensure that the opt-out process is visible and easy to use. The barrage of overdraft marketing makes the option to opt out difficult to miss. Existing accountholders can opt-out easily, by pushing a button on an ATM,[182] clicking a button online, or saying "yes" to a bank employee who calls to suggest to accountholders that they

176 *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY 341, 360 (Jane Winn ed., 2006) (explaining that fewer than 35% of consumers surveyed recalled receiving the financial information privacy notices) (citing Star Systems, *Financial Privacy: Beyond Title V of Gramm-Leach-Bliley,* 2002, at 9).

177 *See* Ben-Shahar & Schneider, *supra* note **Error! Bookmark not defined.**.

178 *See* Ben Popken, *Banks Luring You Into Signing Back Up for High Overdraft Fees*, THE CONSUMERIST (June 18, 2010), http://con.st/10007945; Phil Villarreal, *When it Comes to Overdraft Opt-In, Chase Won't Take No for an Answer*, THE CONSUMERIST (Aug. 6, 2010), http://con.st/10009792.

179 *See* Karen Weise, *Reforms Fail to Halt Bank Revenue on Debit-Card Overdraft Fees*, BLOOMBERG (Oct. 20, 2011), http://www.bloomberg.com/news/2011-10-20/reforms-fail-to-halt-bank-revenue-on-debit-card-overdaft-fees.html; Ben Popken, *Chase Just Goes Ahead and Adds Overdraft Protection to your Account*, THE CONSUMERIST (Sept. 16, 2010), http://con.st/10011137.

180 *See* Villarreal, *supra* note **Error! Bookmark not defined.**.

181 CTR. FOR RESPONSIBLE LENDING, *supra* note 173, at 3–4.

182 *See* Laura Northrup, *Opt In to Overdraft Protection Right at the ATM*, THE CONSUMERIST (July 29, 2011), http://con.st/10021347.

ought to opt out.[183] Any confusion would likely run toward opting out, as banks frame the opt-out position as being a perk that the bank is volunteering to provide, asking accountholders whether they would like to take advantage of the bank's "courtesy pay,"[184] "account protector,"[185] or similarly-named "service." To the extent futility has an effect, it might cut against the default; because consumers can still be charged overdraft fees for checks and automatic debits, consumers trying to avoid overdraft fees might perceive sticking with the default as the futile option. *b. Judgment and Decision Biases.* Firms that benefit from defaults will seek to harness judgment and decision biases to keep consumers in those defaults. But firms that oppose defaults can defuse these biases or even flip them to push consumers out of the default position.

Institutions faced with the financial information defaults work to ensure that these biases support the defaults. For example, one financial institution's opt-out notice appears designed to trigger *loss aversion* and the *endowment effect*. It explains:

> [We are] known for [our] exceptional member service. Sharing member information as we have outlined here enables us to maintain this service excellence . . .
>
> However, federal law also requires that we allow you to opt out . . . Limiting our ability to share financial information . . . will make it difficult for us to serve you as you might expect.[186]

By suggesting that sticking with the defaults will "maintain" the status quo and that opting out will be a departure from what the consumer "might expect," the text suggests that the consumer's expectations—the reference point from which she should measure gains and losses—ought to be the default positions and that opting out will cause her to lose benefits she now has.[187]

Next, financial institutions encourage *procrastination* and *decision avoidance*. The reason the law requires consumers to be given the opportunity to opt out at any time is to reduce transaction barriers. But institutions may emphasize this fact to encourage procrastination[188]—if a consumer can opt out at any time, she need not decide and take action immediately. Further, although framing rules require the opt-out notices themselves to be "reasonably understandable," institutions can make the opt-out decision appear complex and overwhelming. Some institutions offer a plethora of "privacy policies" that consumers must wade through to understand their opt-out rights.[189] Others

183 See sources cited in Willis, U. Chicago article.

184 *Courtesy Pay*, SAN MATEO CREDIT UNION, http://www.smcu.org/accounts/courtesy.php (last visited Aug. 1, 2013).

185 *Sovereign Account Protector*, SOVEREIGN BANK, http://www.sovereignbank.com/personal/promotions/sovereign-account-protector.asp (last visited Aug. 1, 2013).

186 *How to Enable Your Cookies*, *supra* note 175.

187 *See also* Janger & Schwartz, *supra* note **Error! Bookmark not defined.**, at 1243 (discussing specific ways in which financial institutions frame the choice to opt out of the Gramm-Leach-Bliley default as a loss).

188 *Privacy Notice*, CAPITALONE, http://www.capitalone.com/media/doc/corporate/english-privacy-notice.pdf (last visited Aug. 1, 2013) ("You can contact us at any time to limit our sharing").

189 *Privacy Overview*, METLIFE, https://www.metlife.com/about/privacy-policy/index.html?WT.mc_id=vu1179 (last visited Aug. 1, 2013) (listing on its "privacy" webpage: an "Online Privacy Policy," a "Customer Privacy Policy," an

surround the required notice with voluminous "explanations" that are difficult to read and understand.[190] Such complexity encourages procrastination and decision avoidance.

In the face of the overdraft default, on the other hand, banks have waged a masterful marketing campaign designed to negate or reverse the biases that can sometimes make defaults sticky. First, banks reposition *loss aversion* and the *endowment effect* to encourage opting out, using two strategies. One was to pitch opting out prior to the date on which the new legal default rule became effective, thus framing the choice as between keeping an existing endowed position or accepting a change by agreeing to the new default.[191] In their marketing, banks explicitly invoked loss aversion to encourage opting out with copy such as "*Don't lose your ATM and Debit Card Overdraft Protection*"[192] and asking accountholders whether they wanted to "keep [their] account working the same" or "change [their] account."[193] The other is to frame opting out not as losing an endowed position but as gaining the bank's "courtesy pay,"[194] "account protector,"[195] or similarly-named "service" by "opting in."

Second, banks harness *choice bracketing* and play on *discounting* to spur opting out. Consumers are given the choice whether to accept overdraft coverage for any and all ATM and debit transactions that might overdraft the account, rather than on a transaction-by-transaction basis.[196] This broad choice bracketing directs consumers' focus to the question of whether they might *ever* need overdraft coverage (e.g., for an emergency), favoring opting out. If instead, consumers were faced with narrow decisions about whether to accept overdraft coverage and fees for particular transactions, consumers

---

"Auto & Home Privacy Policy," a "HIPAA Notice of Privacy Practices for Personal Health Information," as well as a link for "Opting Out of Information Sharing.").

190 For example, one institution's webpage accompanying its opt-out notice uses the following, over 100-word sentence:

However if you do not want us, your financial advisor or your bank, credit union or other financial institution to disclose your personal information to the New Financial Institution, and if you do not want your financial advisor or your bank, credit union or other financial institution to retain copies of your personal information when your financial advisor or your bank, credit union or other financial institution terminates his, her or its relationship with us, you may request that we, your financial advisor and your bank, credit union or other financial institution limit the information that is shared with the New Financial Institution by filling out the Privacy Choices Notice and mailing it to [address].

LPL Privacy Policy and Opt-Out Information, WEBSTER BANK, https://www.websteronline.com/personal/products-services/investment-services/LPL-privacy-policy.html (last visited Aug. 1, 2013).

191 get cite from U Chicago article

192 *Don't Lose Your ATM & Debit Card Overdraft Protection*, LAPEER COUNTY BANK & TRUST COMPANY, http://www.lcbt.com/2747/mirror/debitcardandatmoverdraftprotection.htm (last visited Aug. 1, 2013).

193 *Stay Protected with Shareplus ATM and Debit Card Overdraft Coverage*, SHAREPLUS FED. BANK, *available at* https://secureforms.c3vault1.com/forms/shareplus/pdf/opt-in-details.pdf (last visited Aug. 1, 2013).

194 *Courtesy Pay*, SAN MATEO CREDIT UNION, http://www.smcu.org/accounts/courtesy.php (last visited Aug. 1, 2013).

195 *Sovereign Account Protector*, SOVEREIGN BANK, http://www.sovereignbank.com/personal/promotions/sovereign-account-protector.asp (last visited Aug. 1, 2013).

196 get cite from U Chicago article

could selectively use overdraft for emergencies and decline it for a cup of coffee. Broad choice bracketing also makes the benefits of opting out appear immediate and certain and the costs delayed and uncertain. Bank advertising includes themes along the lines of "Privilege Pay works like a safety net for your checking account . . . so you don't get left stranded at a gas station"[197]—thus offering accountholders immediate "peace of mind" [198] that funds will be available in an emergency if the consumer opts out.[199] In contrast, banks downplay the costs of overdrafting, emphasizing that opting out of the default and into the bank's overdraft program is a "free" perk and that consumers incur no fee unless they use the "service."[200]

Third, rather than allowing *procrastination*, *decision avoidance*, and *salience* and *omission bias* to lead to inertia, banks place some consumers in a mandated choice scenario and give others deadlines and/or encouragement to act. Some banks require new customers and accountholders attempting to use online banking to make a choice between opting in to the bank's overdraft service or declining that service before they can open an account or continue to use online banking. These accountholders are forced to take action and cannot procrastinate or avoid making the decision. For existing accountholders who do not use online banking, bank marketing frames the decision as one that must be made immediately or by a certain deadline.[201] Bank marketing trumpets "It's your choice!",[202] implying that sticking with the default is a choice, not a blameless omission.

Fourth, banks use explicit messaging so that the *illusion of control* instigates opting out. Bank marketing emphasizes that consumers are "in control" of their overdraft decisions[203] and implies

197 *Privilege Pay*, FARMERS INSURANCE GROUP FED. CREDIT UNION, https://www.figfcu.com/print.php?id=610 (last visited Aug. 1, 2013).

198 *See, e.g.*, *Stay Protected with Shareplus ATM and Debit Card Overdraft Coverage*, *supra* note 193 ("STAY PROTECTED . . . MAINTAIN PEACE OF MIND"); *Sovereign Account Protector*, *supra* note 195 ("Enjoy the peace of mind of knowing your checks, debits, and payments are automatically honored by setting up an Overdraft Protection Plan").

199 *Privilege Pay*, *supra* note 197 ("Privilege Pay works like a safety net for your checking account … so you don't get left stranded at a gas station….")

200 *See, e.g.*, *Overdraft Services*, CAPITALONE, http://www.capitalone.com/bank/overdraft-protection/ (last visited __) ("Opting in is free and easy"); *Check Card Overdraft Protection for your Wescom Checking Account*, WESCOM CREDIT UNION, https://www.wescom.org/accounts/whyoptinoverdraftprotection.asp (last visited __) ("Why Opt in to Check Card Overdraft Protection? It's Free.").

201 *Urgent Notice Regarding Your Public Service Credit Union Debit/ATM Card*, PUBLIC SERVICE CREDIT UNION, https://www.mypscu.com/docs/odpletteronline.pdf (last visited Aug. 1, 2013) ("Urgent notice regarding your . . . Debit/ATM Card. Your immediate response is needed!"); Jim Bruene, *Debit Card Overdraft Protection: 2 Steps Forward, 1.9 Back*, NETBNANKER (July 13, 2010), http://www.netbanker.com/2010/07/debit_card_overdraft_protection_2_steps_forward_19_back.html ("Opt In for Overdraft Coverage on Debit and ATM Cards; August 15 is the deadline to apply if you choose to keep coverage; CLICK HERE TO OPT IN").

202 *See, e.g.*, *Overdraft Services*, CAPITALONE., *supra* note 200.

203 *Overdraft Privilege: Stay Protected*, FIRST FINANCIAL BANK, https://www.bankatfirst.com/personal/spending-account-options/overdraft-privilege-opt-in.aspx (last visited Aug. 1, 2013) ("You now control whether or not you want to continue overdraft privilege coverage for ATM withdrawals and everyday check card transactions.").

that opting out gives consumers more control than sticking with the default.[204] Because the feeling of control encourages riskier behavior, to the extent that consumers understand that they are taking a risk of incurring overdraft fees these marketing messages could encourage them to opt out.

c. Preference Formation Effects. As with transaction barriers and biases, the preference-forming effects of defaults can be bolstered or undermined.

Institutions bolster any advice implicit in the financial information defaults with explicit advice to consumers that their privacy is already protected and they need not opt out.[205] Documents and webpages accompanying the financial information default notices commonly emphasize foremost that the institution cares about the consumer's privacy.[206] For example, although a close read of one institution's required notice reveals that the institution shares consumer information to the fullest extent permitted by law (i.e., with joint marketing partners, affiliates, and non-affiliates, and for both marketing and non-marketing purposes), the webpage from which this notice can be accessed begins boldly: "SAFEGUARDING YOUR PRIVACY" and continues "[WE] TAKE[] OUR COMMITMENT TO PROTECTING YOUR PRIVACY SERIOUSLY".[207]

Institutions explicitly advise consumers that they will benefit by not opting out. For example, one institution explains that sharing information with affiliates provides customers with the following benefits:

> Prevention of unauthorized transactions or fraud.
>
> Account upgrades with additional benefits.
>
> Offers for products and services specifically suited to your individual situation….
>
> Increased convenience, making it faster and easier for you to do business with us….
>
> Enhanced customer service and responsiveness.[208]

The implication is that consumers who opt out of information sharing will not receive these benefits.

In contrast, banks cast the overdraft default so as to negate the preference-forming effects of defaults. Banks typically present accountholders with two checkboxes, one for "opting in" to the bank's "overdraft protection" and another for "opting out," thus concealing which position is the

204 *Overdraft Privilege*, FIRST CMTY. CREDIT UNION, https://www.fccu.org/Resources/PDFs/Overdraft%20Privilege_3_13.pdf (last visited Aug. 1, 2013) ("Keep Your Oversights Under Control"); *Debit Card Overdraft Services*, WEBSTER BANK, https://www.websteronline.com/personal/products-services/checking-services/debit_card_overdraft_services.html (last visited Aug. 1, 2013) ("Giving you control for your everyday debit card purchases.")

205 *See, e.g.*, *Our Privacy Promise to You*, U.S. AUTOMOBILE ASSOC., https://www.usaa.com/inet/ent_references/CpStaticPages?PAGEID=cp_netprivacy_pub (last visited Aug. 1, 2013) ("If you decide that USAA's rigorous practices meet your privacy expectations, **no further action is required**.").

206 *See, e.g.*, *Wells Fargo Privacy and Security*, WELLS FARGO, https://www.wellsfargo.com/privacy_security/privacy/ (last visited Aug. 1, 2013) (begins with "We're committed to protecting your privacy").

207 *Privacy Protection*, CAPITALONE, http://www.capitalone.com/identity-protection/privacy/ (last visited Aug. 1, 2013).

208 *Regions Privacy FAQs*, REGIONS, http://www.regions.com/about_regions/all_facts.rf (last visited Aug. 1, 2013).

default.[209] Further, banks advise accountholders that the opt-out position, rather than the default, is in accountholders' best interests, with copy such as "overdraft privilege is designed with you in mind."[210]

Finally, banks pressed existing accountholders to opt out of the overdraft policy default before it came into effect and they experienced it, and force new customers to make a decision when they open an account. Without living with the default and perhaps discovering that purchases can be foregone or that alternative, cheaper sources of overdraft coverage are available, experience does not induce accountholders to choose the default.

C. SUCCESSFUL DEFAULTS

Of course, many default schemes do work well. Two well-known examples are the above-mentioned retirement savings auto-enrollment default and the Do Not Call registry.

Automatic Enrollment in Retirement Savings Plans: Auto-enrollment allows employers to default employees into participation in defined contribution pension plans at a default contribution rate with a default allocation of investments, rather than waiting for employees to sign up on their own.[211] This policy default scheme is surrounded with framing rules designed to ensure that it is not too sticky, including a requirement that every employee who is enrolled by default be given regular notices of the right to opt out, change their contribution rate, or reallocate their investments. These notices must be written at a level that can be understood by the average employee, so that the opportunity to opt out is not confusing or invisible.[212]

Auto-enrollment has been extremely successful in its goal of increasing the number of employees in the default position. As noted above, employers that have made participation in their plans the default have increased their employee participation rates dramatically.[213] The increase has been largest for lower-income consumers, which has been interpreted as evidence that defaults are most helpful for those who need the most help.[214]

209 *See, e.g.,* First Commerce Credit Union Opt In/ Opt Out Form, *available at* http://www.firstcommercecu.org/accounts_resources/consumer_education/new_regulation_over_draft_protection_options_your_action_is_required/opt_in_opt_out_form#form (stating "Please complete this form to Opt-in or Opt-out of overdraft protection" and then providing two check boxes, one labeled "opt-in" and the other labeled "opt-out").

210 *Overdraft Privilege: Stay Protected*, *supra* note 203.

211 *Retirement Topics – Automatic Enrollment*, INTERNAL REVENUE SERVICE, http://www.irs.gov/Retirement-Plans/Plan-Participant,-Employee/Retirement-Topics---Automatic-Enrollment (last visited Aug. 1, 2013).

212 IRS Income Tax Rule, 26 C.F.R. § 1.401(k)-3(d)(3).

213 *See, e.g.*, Nessmith et al., *supra* note 105, at 6.

214 *See, e.g.*, John Beshears et al., *Public Policy and Saving for Retirement: The "Autosave" Features of the Pension Protection Act of 2006*, *in* BETTER LIVING THROUGH ECONOMICS: HOW ECONOMIC RESEARCH IMPROVES OUR LIVES 274 (John J. Siegfried ed., 2010) (noting "clear and compelling evidence that automatic enrollment was an effective means of increasing savings and improving economic wellbeing, particularly of minorities and of the poor."). This interpretation may be erroneous, as some low-income employees who participate because of automatic enrollment but for whom participation is not optimal. The details of this argument are beyond the scope of this article.

Do Not Call: Another popular default scheme is the Do Not Call Registry. By default, telemarketers can call people to try to sell to them at their homes, but consumers can stop most of these calls by opting out of the default and into the Do Not Call list. The process for opting out of the default and into the Do Not Call list is well known, low-cost and easy—consumers can call a toll-free number or register online.[215] Consumers can opt back into the default wholesale by removing their number from the list, or selectively opt back into the default and allow a particular firm to telemarket to them through written explicit consent.[216] Because this consent must be in writing, the effect is that telemarketers cannot call consumers and convince them to opt back in and then immediately attempt to sell to them.

Although not a penalty default, in that firms do not oppose the default and therefore do not have an incentive to educate consumers, Do Not Call was heavily publicized in the press, and the public responded. Despite having to take some action to opt into the list, consumers placed ten million phone numbers on it in the first four days it was operative,[217] and today over seventy percent of Americans have placed their numbers on the list.[218] Further, it appears that the default sorts consumers reasonably well. Those consumers who do not sign up have the least to gain by doing so, because they tend to receive fewer telemarketing calls; those who have much to gain opt out.[219]

D. CRACKS IN THE THEORY BEHIND THE USE OF DEFAULTS

From the forgoing examples, we can see that defaults are not always sticky or information-forcing. What drives the rift between theory and practice, and why? This section explains why some defaults fail, and then takes this lesson as an opportunity to re-examine the theories behind the use of defaults in policymaking.

215 *FTC Approves Two Reports to Congress on the National Do Not Call Registry*, FED. TRADE COMM'N (Jan. 4, 2010), http://www.ftc.gov/opa/2010/01/donotcall.shtm ("research has consistently shown widespread public awareness of the program and a steady increase in the number of phone numbers registered."); *Register Your Home or Mobile Phone Number*, NAT'L DO NOT CALL REGISTRY, https://www.donotcall.gov/register/reg.aspx (last visited Aug. 1, 2013).

216 Abusive Telemarketing Acts or Practices, 16 C.F.R. § 310.4 (b)(1)(iii)(B)(*i*)

217 *National Do Not Call Registry*, FED. TRADE COMM'N, http://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry (last visited Aug. 5, 2013).

218 As of 2007, 72% of Americans had registered to the list. COUNCIL OF ECONOMIC ADVISORS, 2009 ECONOMIC REPORT OF THE PRESIDENT 244 (2009), http://georgewbush-whitehouse.archives.gov/cea/ERP_2009_Ch9.pdf.

219 Goh Khim-Yong et al*., Consumer Heterogeneity, Privacy, and Personalization: Evidence from the Do-Not-Call Registry* (2009), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.216.44 (providing evidence that consumers in more heterogeneous communities are more likely to sign up for the Do Not Call list, and explaining that this is likely because these consumers receive more telemarketing calls, including more calls marketing goods and services in which they have no interest, because telemarketers cannot target marketing to these consumers as narrowly as consumers living in more homogeneous communities); Goh Khim-Yong et al., *Social Interaction, Observational Learning, and Privacy: the "Do Not Call" Registry*, MPRA Working Paper 8225 (2008) (finding that as telemarketing call volume increased in an area, more households were likely to sign up for the do-not-call list), *available at* http://mpra.ub.uni-muenchen.de/8225/1/MPRA_paper_8225.pdf.

1. Conditions Where Defaults Do Not Work.

The key difference between the automatic enrollment and Do Not Call default schemes on the one hand, and the financial information and overdraft defaults on the other is the presence of parties that have (1) a strong interest in whether the consumer sticks with or opts out of the default and (2) access to consumers so as to shape the presentation of the default and the process for opting out. No party with access to affected employees at the point of the auto-enrollment opt-out decision has a strong interest in pushing consumers in or out of the default. The employers that administer it want it to be sticky, but also do not have a strong reason to try to make it too sticky.[220] Do Not Call has enemies; telemarketers want consumers in the default position.221 But telemarketers do not shape the presentation of the Do Not Call list or the process for signing up; that is run entirely by the Federal Trade Commission. Nor do telemarketers have an effective way to reach consumers whose numbers are on the list to lobby or confuse them into selectively opting back in and permitting the particular firm to telemarket to them, given that consumers must give written, signed consent before a telemarketer can call them.

The financial information and overdraft defaults, on the other hand, are implemented by the firms that want them to fail. Not all financial institutions share customer information with third parties or their affiliates, and not all of those that share with their affiliates allow those affiliates to use the information for marketing purposes. But the institutions that share customer information profit from it and so want to keep their customers in the defaults.[222] Not all banks charge overdraft fees, but many that do profit enormously from them, and thus have every reason to convince accountholders, and frequent overdrafters in particular, to opt out of the overdraft default.[223] Financial institutions and banks both also have access to consumers at the time when consumers can opt out. They each use that access to shape the process for opting out and to frame the default at the point of consumer decision. While the law sets the default itself and some altering and framing rules, the institution or bank makes the last move before the consumer decides whether to opt out.

220 Higher participation levels benefit employers because participation increases employee productivity and retention, particularly for those employees whom employers value more. *See* William E. Even & David A. Macpherson, *Benefits and Productivity*, *in* BENEFITS FOR THE WORKPLACE OF THE FUTURE 43, 48–49 (Olivia S. Mitchell et al. eds., 2003). But where the employer provides a matching contribution, higher enrollment can also be costly for the employer.

221 Telemarketers fought the Do Not Call list for years. *See Mainstream Marketing Services, et al. v. Federal Trade Commission* (10th Cir. 2003), cert. denied.

222 *See, e.g.*, Rupert Jones, *Barclays to Sell Consumer Data*, THE GUARDIAN (June 24, 2013), http://www.theguardian.com/business/2013/jun/24/barclays-bank-sell-customer-data ("Bank tells 13 million customers it is to start selling information on spending habits to other companies"); Catharine New, *Beyond Card Fees: Banks Look to Sell Your Data*, DAILYFINANCE (Oct. 25, 2011), http://www.dailyfinance.com/2011/10/25/beyond-card-fees-banks-look-to-sell-your-data/ ("[Visa and Mastercard] have plans to sell marketers an analysis of anonymous data . . . could be used to create targeted online advertising.").

223 *See* FED. DEPOSIT INSURANCE CORP., FDIC NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS 56 (Dec. 2009), http://www.fdic.gov/householdsurvey/full_report.pd (finding that in 2007, overdraft fees amounted to about 75% of bank deposit account service charges revenue and 25% of total bank noninterest income).

The party opposed to the default is thus able to use its access to powerfully influence the consumer's ultimate position.

2. Re-examining the Theories Supporting the Use of Defaults in Policymaking

The financial information and overdraft defaults suggest that the theories underlying the use of policy defaults, penalty defaults, and even altering and framing rules, are flawed. The theory behind policy defaults is not only that they are sticky for the majority who are better off in the default position, but also that those consumers who truly prefer the opt-out position will opt out. The theory behind penalty defaults is not only that firms will try to convince consumers to opt out, but also that these firms will be forced to educate consumers in the process. The theory behind altering and framing rules is that they can calibrate the stickiness of defaults so that those and only those who ought to opt out do so, and can ensure defaults are information-forcing by requiring the provision of information to consumers before they opt out. But many of these premises are true only if the consumer is well-informed and rational, suppositions at odds with most of the premises behind the use of defaults.

A purely rational actor with known preferences facing a well-understood default and an easy and accessible opt-out position will opt out if and only if she is thereby better off. But given that the mechanisms that make defaults sticky include confusion, biased decision-making, and preference formation effects, and that the uninformed status of consumers is what calls for penalty defaults, it is not clear why those and only those who will be better off in the opt-out position will opt out or why they will be educated in the process of opting out. For example, individuals who do not know they can opt out or who are particularly prone to procrastination may not opt out, even if they would be better off doing so, thus making a default too sticky. In situations of information asymmetry, the more knowledgeable firm may have opportunities to opt out the less knowledgeable consumer without exposing the default. That a consumer finds the decision environment and her own preferences opaque can make a default sticky because this opacity leaves her vulnerable to the mechanisms that can make defaults sticky. But it also means that the default may be too sticky and that she is more susceptible to biased decision-making when those biases run counter to the default position too. A firm opposing a penalty default may find it easier to alter the decision environment so as to push consumer biases to favor opting out than to inform and negotiate with the consumer.

Most altering and framing rules aim to fine-tune transaction barriers or deliver information. But there are two problems with this approach. First, these rules make no attempt to alter the biases and preference formation effects that can make defaults sticky. Second, altering and framing rules meant to alter transaction barriers or be information-forcing may not succeed. For example, not all affirmative actions will inhibit opting out; a reflexive click of a mouse could make a default overly slippery. People often do not read or understand the information presented in legally-required notices.[224] Thus, altering and framing rules are not always information-forcing, and in most instances cannot calibrate the stickiness or slipperiness of defaults well.

224 *See* Omri Ben-Shahar & Carl Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 101 (2011).

III. WHY TRACKING DEFAULTS ARE LIKELY TO FAIL

Currently, transaction barriers, biases, and preference formation effects make the Track-Me position too sticky. Would that change if Track-Me were to become a true policy default, with surrounding altering and framing rules to help those who ought to opt out to do so? To a degree yes, because some existing transaction barriers would be removed. But biases and preference formation effects would likely still give a Track-Me default considerable traction, and firms would likely find ways to erect some transaction barriers without running afoul of altering and framing rules. Moreover, if firms were required to respect a consumer's decision to opt out of a Track-Me default, they would have a stronger incentive to convince consumers not to opt out than they do today. The greater effort firms would expend on keeping consumers in the default could lead fewer consumers to opt out than attempt to do so now.

What if Do-Not-Track were the default instead? Would that lead to consumers sorting themselves into positions that reflect their well-informed preferences? While a Do-Not-Track default would require firms to spend significant resources on maneuvering consumers out of the default, firms determined to do so would likely be successful, without necessarily educating consumers along the way.

Firms that want to track consumers would likely have access to consumers when consumers would face the opt-out choice with respect to that firm and would use that access to push consumers to stick with Track-Me defaults and opt out of Do-Not-Track defaults. The FTC proposal, for example, assumes that in many circumstances, firms that track consumers will be presenting the default and opt-out choices to consumers. Even where consumers can opt out at the browser level or device level, both the W3C draft proposal and the FTC proposal contemplate that consumers who had selected the Do-Not-Track position would be permitted to opt back into tracking by any particular entity by giving consent to that entity directly. Based on strategies firms have used to respond to existing defaults, this Part suggests strategies that firms could use to keep consumers in Track-Me defaults and to lead consumers to opt out of Do-Not-Track defaults. These suggestions are not definitive or exhaustive predictions; firm strategies would of necessity depend on subtle contextual details that cannot be known in advance. But the examples here give the flavor of strategies firms would likely use. This Part then turns to an explanation of why altering rules, framing rules, and competition among firms will not be able to ensure that tracking defaults work well.

A. HOW FIRMS COULD MAKE TRACKING DEFAULTS FAIL

Even with altering and framing rules in place intended to encourage consumers to make well-informed decisions that reflect their preferences, firms will have ample opportunities to make these defaults fail.

1. Erect, Eliminate, or Invert Transaction Barriers

a. Costs: If Track-Me were to become a full-fledged default, firms would attempt to increase the transaction costs that incline consumers toward the default. Regardless of altering rules constraining the cost of opting out, the process would still need to be completed for each browser, program, and device through which the consumer is tracked. If a consumer wanted to vindicate fine-grained

preferences, the number of firms from which the consumer would need to opt out—on each browser on each device the consumer uses—would vastly exceed the number of financial institutions with which consumers might consider exercising their financial information opt-out rights. One reporter counted over 100 companies that tracked her online in a 36-hour period of ordinary web use.[225]

If Do-Not-Track were the default, firms might take a cue from the methods used by banks to convince accountholders to opt out of the overdraft default. When faced with a consumer who has not opted out of a Do-Not-Track default (or who has opted out of a Track-Me default), a website, program, or device might minimize the costs of opting out by offering the consumer a one-click opt-out method. Alternatively, firms might equalize the costs of opting out or sticking with the default by presenting the consumer with two choices—to opt out or not to opt out—and require the consumer to click one of those two before continuing.

Firms could also make opting out of the Track-Me default or failing to opt out of a Do-Not-Track default costly in more tangible ways. First, if legally permitted, firms might give coupons and discounts to those who agree to tracking, making it more immediately and visibly costly to stick with the default than to opt out.[226] Many firms would condition all access to content, apps, and other services on consumers being in the tracked position.[227] When the Netherlands made Do-Not-Track the default for websites, Dutch websites placed a pop-up dialog box between consumers and website content, requiring users to accept all cookies to access the websites.[228] The Dutch Parliament found that these "cookies walls" led to "mindless clicking of 'I accept' buttons."[229]

If the law were to prohibit differential treatment of consumers who do not agree to be tracked, firms might impose subtle costs on consumers who do not agree to be tracked. For example, firms might inundate consumers with marketing that, like the bank opt-out marketing, only stops if the consumer opts out. They might place a complex login process between the website's content and users who are not in a Track-Me position, just as banks require accountholders who have not opted out of the overdraft default to click through a pop-up dialog box asking them to opt out before they can access online banking. Consumers would soon realize that they can avoid the delay of having to click through this screen by agreeing to be tracked, and would soon click "I agree to be tracked" buttons reflexively (meaning it would require more effort to override the reflex and not click the

225 Alexis Madrigal, *Digital Shadow: How Companies Track You Online*, THE WEEK (Apr. 13, 2012), http://theweek.com/article/index/226708/digital-shadow-how-companies-track-you-online.

226 *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1534–35 (2000) (explaining that privacy defaults will not be effective because consumers will sell their personal information too cheaply).

227 *Cf.* Janger & Schwartz, *supra* note **Error! Bookmark not defined.**, at 1244 (noting that if the financial information defaults were changed to prohibit data sharing absent consumer consent, financial institutions would condition services on such consent).

228 Natali Helberger, *Freedom of Expression and the Dutch Cookie-Wall* 2 (Univ. of Amsterdam – Inst. for Info. Law, Working Paper No. ___, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2197251.

229 *Id.* at 4.

button than to click it), just as they click "I have read and agreed to the terms of service" reflexively.[230]

Even more subtle costs and perks are possible. Take a default for behavioral advertising. Rather than contextual advertising (showing consumers ads based on the content the consumer is accessing), firms could show a steady stream of particularly annoying ads (e.g., ads that cover content, ads that take a long time to load and play, ads with lots of distracting movement and noise, ads for unpleasant products) to anyone who is not in the Track-Me position. It might take a bit of time, but consumers would eventually determine that they could avoid these by consenting to tracking.

b. Confusion. Second, firms will have no trouble turning confusion to their advantage. The proposed default schemes under discussion today at the W3C and the FTC consist of a complex mix of Track-Me defaults, Do-Not-Track defaults, and unalterable Track-Me positions, much as overdraft regulation makes no overdraft coverage for ATM and nonrecurring debit transactions the default but permits banks to set overdraft coverage for checks and recurring debit transactions as an unalterable part of consumer checking accounts.

Even if altering rules were to require the opt-out process to consist of a simple, easy-to-use setting change at the browser or device level, firms might place the following choices before consumers: "Click here to opt in to our Privacy Policy" or "Click here to opt out of our Privacy Policy." This is similar to bank overdraft marketing discussed above that asks accountholders to "opt in" to the bank's "courtesy pay" or similarly beneficial-sounding program or "opt out" of the program.[231] Most consumers will assume that a "privacy policy" means that the firm will not share their information.[232] If regulators were to prohibit calling a policy that permits tracking a "privacy" policy, firms would find other confusing labels, such as a "Know Your Customer Policy" or a "Personalized Settings Policy."

Further, regardless of how "clear and conspicuous" framing rules attempt to make a Track-Me default and the option to opt-out, firms will ensure that many consumers do not notice the information, effectively rendering the option to opt-out invisible. It might seem that material on a device screen would be more visible than a fine-print paper financial information opt-out notice that moves quickly from the mailbox to the trash bin. But websites are frequently cluttered material the user is not interested in, and part of the skill of using the web is learning how to mentally screen out this content. Website design is so flexible that even reasonably detailed framing rules about font size,

230 *Cf.* FTC Privacy Report, *supra* note __ at 49 (noting "choice 'fatigue'" problem when web users are repeatedly asked to opt out); Ayres, *supra* note 17, at 2069 (noting the problem that some altering rules are ineffective because people become "habituated to the speed bumps").

231 *Courtesy Pay*, SAN MATEO CREDIT UNION, http://www.smcu.org/accounts/courtesy.php (last visited Aug. 1, 2013); *Sovereign Account Protector*, SOVEREIGN BANK, http://www.sovereignbank.com/personal/promotions/sovereign-account-protector.asp (last visited Aug. 1, 2013).

232 Ilana Westerman, *What Misconceptions Do Consumers Have about Privacy?*, PRIVACY PERSPECTIVES (June 3, 2013), https://www.privacyassociation.org/privacy_perspectives/post/what_misconceptions_do_consumers_have_about_privacy; Jensen et al., *supra* note **Error! Bookmark not defined.**, at 223.

positioning, and the like are unlikely to be effective. COPPA, for example, requires that privacy policies for children's websites be positioned prominently, yet they are frequently surrounded by other materials that draw users' attention away.[233] One set of lab experiments found that while reminding people about privacy increases privacy-protective behavior, even briefly redirecting consumers' attention with a fifteen second delay between the disclosure and the privacy-related choice was enough to negate the effects of the disclosure.[234] Finally, some device screens (e.g., mobile phones) are small, such that some content may not fall within the viewing area, particularly if firms do not want it to fall within the viewing area.[235]

For Do-Not-Track defaults, firms might switch the default rule in the fine print "terms of service." This would make the fact that the consumer has opted out invisible to the consumers who ignore the fine print, and impose transaction costs on those who take the time to read the fine print. In contrast, if altering rules were to require consumers to take an affirmative action to opt out of a Do-Not-Track default, firms would make the process for opting out visible, perhaps even annoyingly so, as banks did with continual reminders that accountholders could opt out of the overdraft default.

c. Futility. Third, consumers likely would not be permitted to avoid all tracking for all purposes; firms will continue to track for "permissible purposes" even those who have opted out. The financial information defaults present the same problem. Even if a consumer has opted out to the fullest extent, financial institutions can continue to share information with joint marketing or other service providers, to share "other" information with affiliates for non-marketing purposes, and "as [further] permitted by law."[236] Just as opting out of sharing in the financial information context, this may leave consumers with a sense that resisting tracking is futile.

2. Harness Judgment and Decision Biases

Salience effects. Firms facing a Track-Me default will no doubt work to keep its salience low, and firms facing a Do-Not-Track default will make the option to opt out salient.

For a Track-Me default, framing rules might increase the salience of the default and opt-out choice somewhat, especially if media coverage of a new law about tracking raises awareness of the possibility of opting out in the abstract. However, firms can easily place an interruption between the provision of any required disclosure about tracking and the consumer's further interaction with the

233 *See, e.g.*, JOSEPH TUROW, PRIVACY POLICIES ON CHILDREN'S WEBSITES: DO THEY PLAY BY THE RULES? (Annenberg Public Policy Center Report 2001) (showing how childrens' websites follow the regulations about the placement of privacy policy links yet are able to surround the links with distracters or otherwise reduce the links' visibility).

234 Idris Adjerid et al., *Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency* 8, *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-sleights-privacy.pdf.

235 *See, e.g.*, FTC Mobile Report at 3 ("[W]ith many devices possessing screens of just a few inches, there are practical challenges in terms of how critical information – such as data collection, sharing of information, and use of geolocation data – is conveyed to consumers.").

236 16 C.F.R. § 313.15 (___).

website or device, diverting consumer attention and destroying the salience of the required disclosure.[237] Even without an interruption, at the concrete moment when consumers are using the app, website, or device, they are likely to be focused on something else, just as a consumer engaging in a financial transaction is attending to the transaction and not the information sharing implications. For a Do-Not-Track default, firms might interrupt consumer use of apps, websites, or devices with pop-up screens or similar barriers so that consumer focus is diverted to the tracking decision. Alternatively, the same repeated presentation of an "I agree to be tracked" button that would lower the transaction costs of opting out by inducing reflexive clicks could also reduce the salience of the option *not* to opt out, in that mindlessly clicking consumers will not give this option consideration.

Omission Bias. Omission bias that favors tracking today would continue to do so under a full-fledged Track-Me default scheme. Given that consumers' current position is generally Track-Me, if this default were imposed, firms could encourage the operation of the bias by emphasizing to consumers that nothing has changed and they need not take any action.

In contrast, firms facing a Do-Not-Track default will work to overcome the omission bias, perhaps by placing consumers in a forced choice scenario, just as banks do with the overdraft default. Without the option to do nothing, omission bias would not favor the default. Even if framing rules prevented firms from forcing consumers to choose between the default and opting out, firms might borrow from bank marketing materials that state or imply that consumers "must" take action, so that inaction no longer appears to be a blameless omission.

Loss Aversion. Under a Track-Me default regime, firms are likely to encourage consumers to treat the default as the reference point against which gains and losses ought to be measured and as the position with which consumers are currently endowed. Just as financial institutions remind consumers that sticking with the default allows banks to "maintain" excellent service and opting out could disrupt that service, firms might characterize Track-Me as the position in which websites, devices, or apps work "properly" or "as you have come to expect" and warn consumers that opting out could impair this functioning.

If a Do-Not-Track default were imposed, firms could copy the marketing strategies used by banks to counter the overdraft default. Firms could frame opting out of the default not as losing an endowed position but as gaining a "personalized" service, just as banks frame opting out of the overdraft default as gaining a service. Given that a Do-Not-Track default would be a change from today's Track-Me world, marketing materials might explicitly invoke loss aversion. Borrowing from bank overdraft marketing, firms might ask: "Would you like to keep" this service "personalized for you?", or "Would you like to change your settings?" Just as banks asked consumers to opt out of the overdraft default before it became operative, under the W3C's proposed scheme, websites or apps can ask consumers to agree to tracking while they are still in the Track-Me position,[238] thus encouraging consumers to view opting out as keeping the status quo. Firms currently tracking

237 *Cf.* Adjerid et al., *supra* note __ at 8.

238 W3C Tracking, supra note __.

consumers might even determine which feature a consumer has used in the past and tailor the marketing to warn the consumer that she "could" lose that feature if she does not opt out.

Procrastination and Decision Avoidance. Making Track-Me a true default leaves intact many of the triggers for procrastination and decision avoidance that lock in the Track-Me position today. Completely opting out would still be a multi-step process, because it would need to be performed on every browser on every device, and again when new browsers or devices are used. Opting out would not stop permissible uses of tracked information, and so consumers uncomfortable with tracking might refuse to think about it long enough to opt out. Firm marketing could encourage procrastination and decision avoidance by reminding consumers that the process requires many steps yet does not stop all tracking. Altering rules could make the opt-out process easier than it is today, but firms will work to ensure that the process still appears difficult. Even if framing rules required that firms provide consumers with brief, easily understandable descriptions of the default and opt-out positions, firms might surround these with voluminous impenetrable "explanations" just as institutions do with respect to the financial information defaults. Copying financial institutions again, firms could encourage procrastination by reminding consumers that they can "opt out anytime."

A Do-Not-Track default would evoke the opposite response from firms. Like banks facing the overdraft default, firms facing a Do-Not-Track default would probably place consumers in a forced choice scenario, such that procrastination and decision avoidance are not options. Firms might also give consumers false deadlines for opting out just as banks do, to reduce procrastination.

Discounting. Facing a Track-Me default, firms would continue to take advantage of the fact that the time and effort costs of opting out, even if small, are immediate, whereas any benefits are uncertain and in the future. To the extent altering rules permit, firms are likely to impose additional immediate tangible costs of consumers who opt out of a Track-Me default, or at least threaten that opting out "might" have such an effect.

If Do-Not-Track were the default, firms could make the potential costs of not opting out seem probable and clear, and promise immediate peace of mind as a benefit of opting out, as banks do with respect to the overdraft default. Imagine a marketing vignette in which a man tries to impress a woman by showing her a photo on his computer screen, but the woman's attention is drawn to advertising that pops up on the man's screen and implies something embarrassing about him. She reacts negatively and he tries in vain to claim innocence. Advertising copy might then ask "Tired of ads that weren't meant for you? Opt into personalized advertising today."

Firms also might downplay the privacy costs of opting out, emphasizing that whatever benefits come with tracking are "free." One can imagine a consumer being asked to opt out of a Do-Not-Track default with the following copy: "Click here to activate Find-My-Phone, a new free service from [your wireless carrier]," accompanied by smaller print that explains that activating "Find-My-Phone" will enable the carrier and its "partners" to geolocationally track the phone.

Choice Bracketing. Firms could try to bracket consumer choices to bolster a Track-Me default. Altering rules likely would permit consumers to opt out at the browser or device level—a broadly-bracketed decision that could lead individuals to make a decision based on the cumulative effect of loss of information privacy, and thus opt out. But firms would then ask consumers to opt back into

the default for "just for this one" firm, website, or app, triggering a narrowly-bracketed decision that favors immediate benefits over privacy concerns.

For a Do-Not-Track default, firms might attempt to force consumers to opt out of *all* tracking to obtain a particular benefit of tracking. This would be similar to bank strategies with respect to overdraft, in that banks generally do not allow consumers to opt out on a transaction by transaction basis but instead require consumers to opt out of the default wholesale in order to obtain overdraft for the emergency that while rare, looms large. On the other hand, firms are unlikely to ask consumers to opt out at the browser or device level—that would benefit the firm's competitors as well as the firm—but instead will seek consent to tracking by that particular firm, and so might emphasize the narrow nature of the opt out decision.

Illusion of Control. Regardless of whether the default is Track-Me or Do-Not-Track, firms could stress to consumers that they are "in control" of their privacy as a way to encourage consumers to take on more risk, just as banks do with respect to overdraft coverage. Here, a legally-enforceable default might give consumers a feeling of greater control than they have today, which ironically could lead to even less privacy-protective behavior. Under a Track-Me default regime, firms could reassure consumers: "You do not need to make a choice now; because YOU are in control of your privacy choices, you can change your settings at any time." Under a Do-Not-Track default regime, firms could reassure them: "Because YOU control your privacy choices, if you no longer wish to receive the benefits of our personalized services, you can always change this setting in the future."

Sunk Costs Fallacy. Under either a Track-Me or a Do-Not-Track default, firms could exploit the sunk costs fallacy to increase the magnetism of the Track-Me position, similar to what occurs with cellphone apps today. Rather than placing tracking walls at the start of a consumer's interaction with a device or program, firms might allow consumers to use the device or program to some extent regardless of the consumer's position. Then, once the consumer has sunk costs into learning to use the device or program, the firm could present a tracking wall to prevent further use. At that point, the fallacy would incline consumers to opt out of a Do-Not-Track position or back into a Track-Me position.

3. Bolster, Undermine, or Reverse Preference Formation Effects

Implicit Advice: If a Track-Me default were adopted, firms would likely channel the implicit advice mechanism to their advantage and bolster it with explicit advice. They could make clear that Track-Me is the default, emphasize that it was set by policymakers in the interests of consumers, and reinforce the endorsement implicit in the default position with explicit advice to stick with the default, as follows:

> Most people don't like receiving a lot of advertising for products they don't want and will never buy. That's why Congress decided to make "Know Your Audience" the

> default for advertising. If you'd like to change this setting, you can. But most people prefer to keep the default.[239]

The reference to Congress makes clear that policymakers set the default to help consumers avoid advertising, and implies that sticking with the default will do just this. Firms might also take the privacy issue on directly and surround any legally-mandated disclosures of the right to opt out with the same tag lines with which financial institutions surround the financial information defaults (e.g., "SAFEGUARDING YOUR PRIVACY" and "[WE] TAKE[] OUR COMMITMENT TO PROTECTING YOUR PRIVACY SERIOUSLY").[240]

In response to a Do-Not-Track default, firms would likely defuse the implicit advice effect by obscuring which position is the default. Just as banks ask consumers to choose between "opting in" to the bank's "overdraft protection" and "opting out,"241 firms might ask consumers to select between "opting in" to the firm's "privacy policy" (where that policy effectively opts the consumer out of the Do-Not-Track position) or "opting out" (where "opting out" means sticking with the Do-Not-Track default). Firms could also counter any implicit advice with explicit advice to opt out of the Do-Not-Track default. Firms might suggest that their "privacy" policies were developed with [the consumer's] needs in mind and advise consumers that if they opt into the firm's privacy policy, they "can rest assured" that their "privacy will be respected." Explicit advice is likely to speak louder than implicit advice.

Experience: For Track-Me defaults, firms would likely emphasize that nothing has changed and the consumer can continue to use the program or device as she has always done if she sticks with the default. Because any Do-Not-Track position would be a change, firms would likely push consumers to opt out before that change became effective, as banks did with the overdraft default. This would prevent consumers from experiencing the default and potentially developing a preference for it.

* * * * *

Some of the strategies discussed above are at cross-purposes. For example, on the one hand, reminding people that they *control* their own position might encourage risk taking and thus sticking with a Track-Me default. On the other hand, "you are in control" marketing might make salient that consumers are *responsible* for their own positions, and thus discourage omission bias that would otherwise favor sticking with a Track-Me default. If a full-fledged tracking default scheme were adopted, firms would gradually refine their marketing through testing a variety of campaigns, potentially even using data gleaned from tracking to target their approaches.[242]

---

239 "Most people" plays off the tendency of consumers to follow the crowd with respect to privacy behavior. Referring to opting out as a "change" reinforces biases favoring the status quo. "Know your audience" sounds like a duty placed on firms, which is likely to be more attractive to consumers than "Track-Me," which sounds like an imposition on consumers.

240 *See* note 215, *supra. (Privacy Protection*, CAPITALONE)

241 *See supra* note _217_ (First Commerce Credit Union Opt In/ Opt Out Form).

242 *See* Ryan Calo, *Taking Data Seriously: Market Manipulation in the Digital Age*, YALE LAW SCHOOL INFO. SOC'Y PROJECT (Mar. 28, 2013), http://www.yaleisp.org/event/thomson-reuters-speaker-series-ryan-calo.

B. ALTERING RULES, FRAMING RULES, AND COMPETITION

1. The Limits of Altering and Framing Rules

Firm ploys to increase or decrease the stickiness or slipperiness of defaults might seem to be easily countered with altering and framing rules. For example, to make defaults stickier, policymakers might impose costly opt-out procedures. To prevent firms from making defaults too sticky, policymakers might prohibit conditioning transactions on, or giving perks for, sticking with a default. Policymakers might require specified disclosures crafted to frame the default and opt-out positions in ways that harness or defuse biases. Or policymakers might require disclosures that convey explicit advice about whether consumers ought to stick with the default or opt out. But normative, legal, and practical constraints limit these rules.

a) Respect for Heterogeneous Preferences

A default regime rather than a mandate for personal information tracking is premised on the idea that consumers have heterogeneous preferences regarding privacy and the benefits tracking can provide, and that the law should respect that heterogeneity by allowing consumers to decide for themselves whether to be tracked.

As a normative matter, altering rules that substantially inhibit opting out are inconsistent with respect for individual tracking preferences. For example, reverting defaults that require consumers to opt out every time they open up their browsers or fire up their mobile devices[243] might effectively keep consumers in the default position (provided that firms did not manage to make the opt out process so easy and routine that consumers would opt out mindlessly[244]), but would be difficult to justify normatively. Even prohibiting differential treatment of consumers depending on whether they have agreed to be tracked,[245] while it could prevent the most blatant ways that firms might maneuver consumers into agreeing to tracking, might also be normatively problematic. Where tracking currently funds the provision of the website, app, or device at issue, such a rule could have substantive effects on the availability of these to consumers, particularly consumers that lack financial means to pay with cash. Such substantive effects may be an appropriate trade-off for increased information privacy, but go beyond merely giving consumers notice and informed choice about tracking.

243 *Cf.* Paul Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2098-2017 (2003-2004) (proposing a default rule that a consumer's personal data cannot be transferred to third parties, complemented by altering rules requiring that the consumer consent to each subsequent transfer of her data at the time the data is transferred, with the aim that the default would be sticky).

244 *Cf.* Yang Wang et al*., supra* note **Error! Bookmark not defined.** ("Some of our participants reported that they began to ignore our nudges after several days. Future work might investigate addressing this habituation effect . . . .").

245 *See* Paul M. Schwartz & Daniel Solove, *Notice & Choice: Implications for Digital Marketing to Youth*, Memo prepared for the 2nd NPLAN/BMSG Meeting on Digital Media and Marketing to Children (2009), *available at* http://digitalads.org/documents/Schwartz_Solove_Notice_Choice_NPLAN_BMSG_memo.pdf (proposing altering rules prohibiting "mak[ing] the provision of access, information, services, or transactions contingent upon a person's" consent to tracking).

Framing rules that would be dramatic enough to be effective are also normatively problematic. In a world cluttered with information and decisions, commanding attention requires something more drastic than a neutral description of the default and opt-out positions, such as those currently required for the financial information defaults. But imagine a mandated disclosure likening tracking to stalking or spying, conveyed through pictures along the lines of the graphic cigarette warnings recently proposed by the Food and Drug Administration.[246] While potentially effective in convincing consumers to stick with a Do-Not-Track default, this disclosure would be incompatible with an aim by policymakers to allow people to sort themselves into their desired positions freely, with no policymaker push in any particular direction.

Framing rules that require more complex disclosures or other forms of consumer education might be another strategy, one that could in theory reduce consumer preference uncertainty that fuels susceptibility to firm framing manipulations. But in a quickly changing, complex decision environment, the utility of such education is likely to be nil.[247] Only simple, easily actionable messages tend to be effective in public education campaigns.[248] But a policymaker who believes that consumers ought to take a variety of positions with respect to tracking cannot send a simple "just say no" or "just say yes" message.

b) Mis-sorting

A further obstacle to developing more effective altering and framing rules is a practical one—most such rules are unlikely to sort consumers well. Consider an altering rule designed to counter firm manipulation by making it more difficult for a consumer to opt out of a Do-Not-Track position, without preventing opting out entirely, such as a rule requiring a consumer to send a signed letter through the U.S. Postal Service. Consumers who are in the habit of using traditional mail would find this altering rule no more than a speed bump, whereas consumers who conduct their lives on-line are more likely to be impeded by such a rule. Yet there is no reason to think that more members of the former group ought to opt out (that is, ought to be tracked) than the latter. Or consider a requirement that consumers pass an on-line test of understanding of the default and opt-out positions as a condition of opting out. Although this process might be informative to those who completed it, many consumers dislike being tested and would be deterred from attempting to opt out on this basis. Others have weak reading or comprehension abilities that would impair test performance. Yet consumers who dislike or perform poorly on written tests are not less likely to benefit from opting out than consumers who enjoy and perform well on written tests.

c) Commercial Speech Doctrine Limits

Given the likelihood that firms will engage in marketing that drives judgment and decision biases to favor the Track-Me position, framing rules prohibiting this type of marketing might seem an

246 *See, e.g.*, *R.J. Reynolds Tobacco Co. v. Food & Drug Admin.*, 696 F.3d 1205, 1221–22 (D.C. Cir. 2012) (describing the Food and Drug Administration's proposed cigarette warnings).

247 *Cf.* Lauren E. Willis, *Against Financial Literacy Education*, 94 IOWA L. REV. 197 (2008).

248 *See* Jessica Aschemann-Witzel et al., *Lessons for Public Health Campaigns from Analysing Commercial Food Marketing Success Factors: A Case Study* 9 (BioMed Central Public Health 2012).

appropriate response. Alternatively, framing rules might, in theory, require firms to frame the default and opt-out positions in particular ways.

Under current First Amendment doctrine, commercial speech has a substantial degree of protection.[249] Framing rules generally cannot prohibit firms from using particular speech, graphics, or vignettes to convey commercial messages if those messages are not misleading.[250] Although telling consumers they will not be tracked when they are being tracked is misleading,[251] none of the firm marketing ploys described above would likely be found misleading. The government is also limited in the disclosures that it can require firms to make. For example, while a disclosure likening tracking to stalking or spying might be effective in convincing consumers to stick with a Do-Not-Track default, forcing firms to give such a disclosure might violate current constitutional limits on the regulation of commercial speech.[252]

Without the ability to prevent firm speech that frames the default and opt-out positions or to require disclosures that can reach consumers through dramatic messages, firms have the upper hand; they can better reach the consumer at the point of decision and can frame the decision using anything short of demonstrably misleading speech.

d) The Last Mover Wins

Finally, practical limits on regulation will inhibit policymakers' efforts to manipulate consumer judgment and decision biases or prevent firms from doing so. True, firm ploys to keep consumers in Track-Me defaults, move them out of Do-Not-Track defaults, or move them back into Track-Me defaults will sometimes fall flat or even backfire. Consumers are a diverse and fickle lot; what one consumer finds acceptable another finds out-of-bounds, and a single consumer might find a path-breaking firm's actions disquieting at first but unremarkable if the rest of the market moves in the same direction.[253] But firms can send a diverse set of marketing messages (informed by behavioral

249 Any governmental restriction on nonmisleading commercial speech must (1) "directly advance" a substantial governmental interest and (2) be "narrowly tailored" to serve that interest. *See* Central Hudson Gas & Electric Corp v Public Service Commission of New York, 447 US 557, 564 (1980).

250 *See* Willis, *supra* note __ at __ (explaining how current commercial speech doctrine restricts rules prohibiting firm framing manipulations) (Chicago piece).

251 *See* ScanScout Order, *supra* note __.

252 *See id.* at __ (explaining how current commercial speech doctrine prevents the government from requiring firms to give consumers dramatic notices).

253 For example, Google's February 2012 privacy policy allowing third-party data sharing was met with controversy, but few noticed when Microsoft followed suit in October after running the "Scroogled" campaign criticizing Google. Jeff Blagdon, *Google's Controversial Privacy Policy Now in Effect*, THE VERGE (Mar. 1, 2012), http://www.theverge.com/2012/3/1/2835250/google-unified-privacy-policy-change-take-effect; Edward Wyatt & Nick Wingfield, *As Microsoft Shifts its Privacy Rules, an Uproar is Absent*, N.Y. TIMES (Oct. 19, 2012), http://www.nytimes.com/2012/10/20/technology/microsoft-expands-gathering-and-use-of-data-from-web-products.html?pagewanted=all&_r=0.

tracking data), and only need one of these to work with any particular consumer. Firms can also experiment with risky approaches on a small scale, and can change course quickly.[254]

Policymakers are not nearly so agile. For example, policymakers might require that consumers be given disclosures that frame opting out of the default position as a loss.[255] But firms can run circles around disclosures.[256] Policymakers can set altering rules, but firms implementing those rules have the final say on how the entire opt-out process is designed.

The legal rules can be put in place, but firms can simply work around them. An altering rule does not set how the default will be altered; it merely sets one aspect of that process, and firms control the rest, yet it is the entire process that affects the stickiness or slipperiness of the default. A framing rule can control one aspect of a frame, but firms can place that aspect within a larger frame that determines how effective the legal framing will be. If the law could respond to each firm maneuver—and then hold everything constant—altering rules and framing rules might be able to fine-tune the power of a default. But the law cannot require stasis.

2. Will Competition Change the Calculus?

Is it possible that competition could do what government regulation cannot, creating a robust market for privacy, complete with consumers who make well-informed decisions about tracking that reflect their preferences? One can imagine the pitches: "With our cellphone, no one can track you"; "Google tracks you. We Don't."[257]; "We're a social network, not an advertising network."[258] Firms seeking to compete based on promises not to track consumers would not be limited by the normative, political and constitutional constraints facing lawmakers. They could unabashedly press the merits of privacy and the demerits of tracking and could respond quickly to their competitors' marketing strategies with their own attempts to bend consumer judgment and decision biases to their favor. But will they? And if so, does the default matter?

254 *Cf. Facebook Backs Down, Reverses on User Information Policy*, CNN (Feb. 18, 2009), http://www.cnn.com/2009/TECH/02/18/facebook.reversal/. *See also* Calo, *supra* note __.

255 *Cf.* Janger & Schwartz, *supra* note **Error! Bookmark not defined.**, at 1259 (proposing mandatory language for financial information default opt-out notice that attempts to invoke loss aversion to favor opting out by warning that if a consumer does not opt out within 30 days, the institution may start sharing her data, and "ONCE WE HAVE SHARED INFORMATION WITH OTHER COMPANIES, WE CANNOT GET IT BACK FROM THEM OR STOP THEM FROM USING IT" (based on notice suggested by Public Citizen)).

256 *Cf.* David A. Hyman & David J. Franklyn*, Search Neutrality and Search Bias: An Empirical Perspective on the Impact of Architecture and Labeling*, (Ill. Program in Law, Behavior and Soc. Sci., Paper No. LE13-24, Univ. of S.F. Law, Research Paper No. 2013-15, 2013), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2260942 (finding that labeling search engine in particular ways has no effect on consumers but changing the architecture of results can be effective).

257 Kunur Patel, *How Do You Brand Consumer Privacy?*, ADAGE (Feb. 13, 2012), http://adage.com/article/digital/brand-consumer-privacy/232694/ (quoting advertising copy used by internet search engine DuckDuckGo).

258 *Cf.* Todd Bishop, *Microsoft Releases IE10 For Windows 7, Sticks To Its Guns On 'Do Not Track'*, GEEKWIRE (Feb. 26, 2013), http://www.geekwire.com/2013/microsoft-releases-ie10-windows-7-auto-updates/ (describing Microsoft's use of a Do-Not-Track default in Internet Explorer 10 as a marketing bid to gain browser market share).

Although some privacy-based competition has appeared in the marketplace, thus far it appears of limited effectiveness. A small cadre of privacy sophisticates may choose websites, apps, and devices based on reliable promises not to track consumers, but most consumers have difficulty distinguishing firms and products on privacy grounds.[259] Competition appears to be over privacy image rather than privacy reality.[260] For example, while the TRUSTe privacy certification seal increases consumer trust in websites,[261] one study found that websites using this seal engage in more privacy-invasive practices than firms without the seal.[262] Microsoft's recent "Scroogled" marketing campaign, which paints Google as a privacy-invader[263] may turn out to be mere optics; Microsoft's campaign criticizes Google for tracking consumers, but Microsoft also reserves the right to track consumers in the fine print of its contracts.[264] Consumers who realize that privacy marketing is an unreliable indicator of privacy practices may treat the situation as a lemons market and assume all firms track them.[265]

A legal default might change this dynamic somewhat, particularly a Do-Not-Track default that required firms to obtain express consumer consent before tracking. In effect, a firm requesting consent would be admitting that it is trying to track consumers, an admission that might be clearer to consumers than those found today in unread privacy policies. Such an admission might help consumers distinguish firms based on the firms' tracking practices, a predicate for genuine privacy-based competition.

259 *Cf.* Joseph Bonneau & Sören Preibusch, *The Privacy Jungle: On the Market for Data Protection in Social Networks*, *in* The 8th Workshop on the Economics of Information Security (2009), http://preibusch.de/publications/Bonneau_Preibusch__Privacy_Jungle__2009-05-26.pdf (finding that the "economically rational choice for a [social networking] site operator is to make privacy control available to evade criticism from privacy fundamentalists, while hiding the privacy control interface and privacy policy to maximise sign-up numbers and encourage data sharing from the pragmatic majority of users.").

260 Patel, *supra* note 257 (describing widespread advertising by web firms, including Google, touting their privacy-protectiveness); Joseph Turow, *Behavior Aside, Consumers Do Want Control of Their Privacy*, ADAGE (Jan. 29, 2013), http://adage.com/article/guest-columnists/behavior-consumers-control-privacy/239376/ (demonstrating how firm marketing may convince consumers that they are protecting consumer privacy even when a closer read of privacy policies reveals this protection to be minimal).

261 Jensen et al., *supra* note **Error! Bookmark not defined.**.

262 Benjamin Edelman, *Adverse Selection in Online 'Trust' Certification*, in International Conference on e-Commerce (2009).

263 Michael Learmonth, *Microsoft Debuts New Commercials on Privacy, With Google in the Crosshairs; Bringing up Privacy to Draw a Distinction With Rival*, ADAGE, (Apr. 22, 2013,) http://adage.com/article/digital/microsoft-launches-privacy-tv-campaign-google-crosshairs/241001/ (describing Microsoft's use of privacy in its marketing to distinguish itself from Google, and noting that "ad-supported web services are a money-losing side show for Microsoft but a profitable core business for Google."); Geoff Duncan, *Why Do Not Track May Not Protect Anybody's Privacy,* DIGITAL TRENDS (June 9, 2012), http://www.digitaltrends.com/mobile/why-do-not-track-may-not-protect-anybodys-privacy/ (suggesting that Microsoft set Do-Not-Track as the default for IE 10 both as a marketing strategy and to undercut Google's advertising revenue).

264 Strange, *supra* note **Error! Bookmark not defined.**.

265 Tony Vila et al., *Why We Can't Be Bothered to Read Privacy Policies*, *in* ECONOMICS OF INFORMATION SECURITY 143 (L. Jean Camp & Stephen Lewis eds., 2004) (explaining how privacy market functions like a lemons market).

But because the returns to firms from tracking are only likely to grow,[266] it is likely to be more profitable for most firms to join the trackers rather than compete against them based on privacy. For example, online retailers might want consumers to stay in a Do-Not-Track position with respect to geolocational cellphone tracking to prevent their brick-and-mortar competitors from using this tracking to attract market share. However, online retailers are likely to want to use internet use tracking for their own purposes. Marketing that encourages consumers to adopt a Do-Not-Track position for geolocational tracking could imperil marketing efforts to keep consumers in a Track-Me default on the internet.

While it is impossible to know whether a robust privacy market will develop, the "cookie wall" experience in the Netherlands is instructive. Dutch law made plain which firms were tracking consumers online because only those firms had to ask consumers to opt out of the Do-Not-Track default.267 But virtually all firms (and even nonprofits[268]) responded to the law by requiring consumers to opt out as a condition of using the firm's website, not by competing on promises not to track.[269]

IV. CONSEQUENCES OF PRIVACY POLICY BY DEFAULT

None of this tells us whether or when Track-Me or Do-Not-Track is the best position for some or all consumers to be in. The benefits to society of tracking certainly exceed the costs in some situations. But a default scheme surrounded by firm manipulations intended to keep consumers in or spur consumers to the Track-Me position creates only the façade of choice, and that façade cannot justify the conclusion that Track-Me is the right position. To assess whether and when consumers ought to be tracked would require a far more difficult inquiry than checking whether a consumer has clicked a button opting out.

Privacy by default seems like an elegant, low-cost way to resolve concerns about personal information tracking without imposing positions on consumers. Leaving tracking decisions to individual consumers also sidesteps difficult tradeoffs between incommensurate values and politically perilous substantive judgment calls that policymakers would rather not make. If all policymakers are aiming for with a notice-and-choice regime of information privacy defaults is to avoid political heat, they may succeed. But if they seek to use tracking defaults as a way to set norms, guide consumers to individually or socially desired positions, or inform consumers through the opt-out decision process, they are likely to fail.

266 *See, e.g.*, James Temple, *Rules Against Tracking Don't Go Far Enough*, SAN FRANCISCO CHRONICLE, Mar. 7, 2012,, available at http://www.sfgate.com/business/article/Rules-against-online-tracking-don-t-go-far-enough-3387373.php ("Targeting ads based on search queries, sites visited, stories read and social connections forms the core of the multimillion-dollar business models of many online companies, including Google, Yahoo and Facebook.").

267 *See* Helberger, *supra* note 228.

268 *See, e.g.*, *Cookies*, TUDelft, http://cookie.tudelft.nl/index.php?action=verify&origin=http://home.tudelft.nl/en/ (last visited Aug. 1, 2013).

269 *See* Helberger, *supra* note 228.

More generally, nudges may not be an effective way to help people make better choices about information privacy. Nudges can be powerful when no one is pushing back. But a push can easily overwhelm a nudge. Existing research showing such nudges to be effective is performed in artificial conditions in which no firm that opposes the nudge has an opportunity to intervene.270 But firms can use the same mechanisms and conditions that make nudges work to make nudges fail. That nudges work in the lab shows that people's privacy decisions are heavily influenced by framing– which, ironically, is some evidence that nudges may not work in practice, given that firms can reframe nudges. For these experiments to have the external validity necessary to inform public policy, researchers must anticipate and account for the dynamic responses of firms to the proposed nudges.[271]

Yet the broader effects of tracking defaults on the politics of information privacy are uncertain. On the one hand, tracking defaults could be a useful, collectively educative political way station on the road to better information privacy regulation. A default makes tracking more visible than it would be were Track-Me the only option. While tracking defaults are unlikely to directly lead individuals to make well-informed decisions, at the societal level, defaults could foment discussion and debate that inform the populace.[272] In turn, this could create political pressure for better regulation.

On the other hand, Do-Not-Track defaults might delay or derail better information privacy regulation, for two reasons.

First, by creating the façade of robust choice, courts, commentators, and consumers themselves are more likely to blame consumers for any adverse consequences that might flow from sticking with the default or from opting out. Experience with opting out of the civil justice system is instructive here. Some sellers, after placing a clause opting out of the civil justice system and into arbitration in the fine print of their standard form consumer contracts, then permit consumers to "opt out" of the waiver (and thus opt back into the legal default) while keeping the good or service.[273] These firms have apparently calculated that the costs to the firms of the few consumers

270 See, e.g., Rebecca Balebako et al., *Nudging Users Towards Privacy on Mobile Devices*, *in* Proceedings of the 2nd International Workshop on Persuasion, Influence, Nudge & Coercion Through Mobile Devices (2011); M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027 (2012); Yang Wang et al., *"It made me think twice": A Field Trial of a Facebook Privacy Nudge*, Paper in the Privacy Law Scholar Conference (2013); Alessandro Acquisti, *Nudging Privacy: The Behavioral Economics of Personal Information*, 7 IEEE 82 (2009).

271 As explained above, the one set of lab experiments that aimed at external validity by briefly redirecting consumers' attention away from a disclosure intended to nudge the consumer to engage in privacy-protective decisions, just as firms can be expected to redirect consumer attention from any required disclosure of the option to opt out of a Track-Me default, found that even a very brief distraction was enough to negate the effects of the disclosure. Aderjid et al, *supra* note __.

272 *Cf.* David Adam Friedman, *Micropaternalism*, 88 TUL. L. REV. (forthcoming 2013) (making similar argument about supersize soda bans and their impact on discussion and debate about food and health, even if the bans fail in the courts).

273 *See, e.g.*, *Discover Gift Cardholder Agreement 2010*, DISCOVER CARD, http://www.discovercard.com/shopcenter/giftcard-terms.shtml (last visited Aug. 1, 2013); *Comcast Agreement for Residential Services*, COMCAST, http://www.comcast.com/Corporate/Customers/Policies/SubscriberAgreement.html (last

who will actually exercise this choice are well worth the benefits the firms receive. These benefits could include deterring self-blaming consumers from challenging the fine print clauses, convincing courts that the contracts cannot be unconscionable if consumers can opt out of these clauses,[274] or arguing in the political process that substantive regulation of these clauses is unnecessary because consumers can opt out. So too in the privacy realm, Track-Me defaults with which consumers stick en masse and Do-Not-Track defaults from which consumers opt out en masse might defuse pressure, whether directly from consumers or through the courts or the political process, for more meaningful reform.

Second, a notice-and-choice regime of defaults not only reflects the current understanding of privacy as an individual choice, but re-inscribes it. The model conveys the message that the problem is one of accommodating heterogeneous consumer privacy preferences or heterogeneous consumer calculi about the right tradeoff to make between their privacy preferences and the value they place on the benefits tracking can provide. Other conceptions—for example, as a conflict between the privacy required for individual experimentation, reflection, and flourishing necessary for innovation and a liberal democratic society[275] and the utility of the free flow of personal information to society[276]—might lead to different policy responses. But it may be that so long as privacy continues to be understood as a right of individuals "to determine for themselves when, how, and to what extent information about them is communicated to others,"[277] better forms of regulation will remain unimagined.

visited Aug. 1, 2013); *T-Mobile Terms & Conditions*, T-MOBILE**,** http://www.t-mobile.com/Templates/Popup.aspx?PAsset=Ftr_Ftr_TermsAndConditions&print=true (last visited Aug. 1, 2013).

274 This move has been successful in some courts. *See, e.g.*, *Edelist v. MBNA Am. Bank*, 790 A.2d 1249, 1258 (Del. Super. Ct. 2001) (holding that a consumer's failure to avail himself of firm-dictated opt-out provisions mean arbitration clause is binding); *Hoefs v. CACV of Colorado, LLC*, 365 F. Supp. 2d 69, 73–74 (D. Mass. 2005) (same).

275 *See, e.g.,* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013) (arguing that privacy is necessary for both innovation and democracy);; Allen, *supra* note **Error! Bookmark not defined.**; Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VANDERBILT L. REV. 1607 (1999)..

276 *See* Tene & Polonetsky, *supra* note 6.

277 WESTIN, *supra* note **Error! Bookmark not defined.**, at 7.